Atlantic Council

IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE
DE L'ÉCOLE MILITAIRE

The "Macron Leaks" Operation: A Post-Mortem

Jean-Baptiste Jeangène Vilmer

The "Macron Leaks" Operation: A Post-Mortem

Jean-Baptiste Jeangène Vilmer

ISBN-13: 978-1-61977-588-6

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The author is solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

June 2019

Contents

Acknowledgments

This report is the result of a joint effort between the Atlantic Council’s Digital Forensic Research Lab, Eurasia Center, and Future Europe Initiative, and the Institute for Strategic Research (IRSEM) at the French Ministry of the Armed Forces as a part of joint efforts to combat disinformation.

Earlier versions of parts of this report have been previously published in *Successfully Countering Russian Electoral Interference: 15 Lessons Learned from the Macron Leaks*, *CSIS Briefs*, Washington, DC, June 21, 2018; *Information Manipulation: A Challenge for Our Democracies*, a 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 of the Armed Forces, Paris, August 2018; and “Lessons from the Macron Leaks,” in *Hacks, Leaks and Disruptions: Russian Cyber Strategies*, EUISS, Chaillot Paper No. 148, eds. Nicu Popescu and Stanislav Secrieru, October 2018, 75-83.

The opinions expressed in this report are my own and do not represent an official position of the Ministry of the Armed Forces or the Ministry of Foreign Affairs. I would like to thank Paul Charon, François Delerue, Louis Gautier, Ben Nimmo, and Boris Toucas for their valuable comments on earlier drafts.

Abstract

Among the long list of electoral interference attempts in recent years, one case is especially important to study: the 2017 French presidential election, because it failed. It failed in the sense that the result of the election did not coincide with the aim of the attackers. There was a coordinated attempt to undermine Emmanuel Macron’s candidacy, with a disinformation campaign consisting of rumors, fake news, and even forged documents; a hack targeting the computers of his campaign staff; and, finally, a leak—15 gigabytes (GB) of stolen data, including 21,075 emails, released on Friday, May 5, 2017—just two days before the second and final round of the presidential election. This leak was promoted on Twitter by an army of trolls and fake accounts (bots), with the hashtag #MacronLeaks appearing in almost half a million tweets in twenty-four hours, and so the attack is now remembered as “the Macron Leaks.” However, the leak itself was only the pinnacle of a coordinated operation that started months before, with a disinformation campaign and a hack. Therefore, we should rather speak of a “Macron Leaks” operation, which did not sway French voters and change the result. Winning 66.1 percent of the vote, Macron defeated Marine Le Pen, the far-right candidate. The aim of this report is to provide the most detailed single account to date of the “Macron Leaks” operation. With the benefit of hindsight, it explores what happened, who (likely) orchestrated the affair, how it was successfully countered, and what lessons can be learned. In conclusion, it will also explain what France has accomplished since then in order to fight information manipulation and what is yet to be done.

Introduction

Foreign electoral intervention is nothing new. For as long as elections have existed, foreign powers have attempted to influence them, overtly or covertly, in order to help or hinder one candidate (partisan electoral intervention) or simply to weaken the democratic process itself, irrespective of who wins (process electoral intervention).[1] In recent years, however, foreign electoral intervention has been made easier by the exponential development of digital platforms and the correlative increased risk of information manipulation.[2] As analyst Ben Nimmo has written, “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.”[3] Those facts, combined with structural factors (a crisis of confidence in institutions, rejection of the elites, polarization of identity, crisis of the press, etc.), partly explain the range of interference in democratic processes in the last years: the 2016 Dutch referendum on the association agreement between Ukraine and the European Union (EU), the 2016 United Kingdom’s referendum on membership in the European Union (which resulted in Brexit), the 2016 American presidential election, the 2017 French presidential election, the 2017 German federal elections, the 2018 Irish abortion referendum, and the 2018 Taiwanese local elections, among others.

Another part of the explanation is geopolitical. In most of these cases, Russia stands accused. Electoral interference appears to be one of Russia’s many tools to increase its influence on the world stage. Russia’s return to prominence has been gradual and multiform since 2008, with its military intervention in Georgia, followed by a military modernization, the annexation of Crimea (2014), military interventions in Ukraine and Syria (since 2015), and a growing political, diplomatic, military, and economic footprint in the Middle East and Africa. President Vladimir Putin, who famously called the collapse of the Union of Soviet Socialist Republics (USSR) “the greatest geopolitical catastrophe of the 20th century,” makes no secret of his ambition to restore Russia’s grandeur. To that end, Moscow developed an offensive interpretation of soft power: in its 2013 Concept of Foreign Policy plan, it mentions the “risk” that soft power can be used “to exert political pressure on sovereign states, interfere in their internal affairs, destabilize their political situation, manipulate public opinion”[4]—implying that the risk is *to* Russia. 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. However, to “defend” itself, it developed a highly offensive interpretation of soft power. In 2009, the Russia Today TV channel was renamed RT and shifted its approach from promoting Russia, which was unsuccessful, to discrediting the adversary.[5] Since the Ukrainian crisis in particular, the Kremlin has strengthened its information offensive toward states in its “near abroad” and the West. Since 2016, these techniques have grown more sophisticated 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,” as well as the extension of the National Guard’s jurisdiction over the informational and cyber fields.[6]

Russia is certainly not the only actor potentially involved in foreign electoral intervention: in the case

[1] Daniel Corstange and Nikolay Marinov, “Taking Sides in Other People’s Elections: The Polarizing Effect of Foreign Intervention,” *American Journal of Political Science* (July 2012), 655-670. See also Stephen Shulman and Stephen Bloom, “The legitimacy of foreign intervention in elections: the Ukrainian response,” *Review of International Studies* (2012), 445-471; Dov H. Levin, “When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results,” *International Studies Quarterly* (2016), 189-202; Dov H. Levin, “A Vote for Freedom? The Effects of Partisan Electoral Interventions on Regime Type,” *Journal of Conflict Resolution* (2018), 839-868; Paul Baines and Nigel Jones, “Influence and Interference in Foreign Elections,” *The RUSI Journal* (2018), 12-19.

[2] Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, Janaina Herrera, *Information Manipulation: A Challenge for Our Democracies*, Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry of the Armed Forces, August 2018, https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

[3] Written Representation 36, Singaporean Parliament, Select Committee on Deliberate Online Falsehoods–Causes, Consequences and Countermeasures (February 22, 2018) (testimony of Ben Nimmo, senior fellow for information defense, Atlantic Council Digital Forensic Research Lab).

[4] Ministry of Foreign Affairs of the Russian Federation, *Concept of the Foreign Policy of the Russian Federation* 2013, para. 20.

[5] Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money, The Interpreter, The Institute for Modern Russia*, 2014, 15, https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf.

[6] Canadian Security Intelligence Service, *Who Said What? The Security Challenges of Modern Disinformation, World Watch: Expert Notes*, series publication No. 2018-02-01, February 2018, 35.

French President elect Emmanuel Macron and his wife Brigitte celebrate on the stage at his victory rally near the Louvre in Paris. *Photo source: Reuters*

of the 2018 Taiwanese election, for instance, China is suspected.[7] And non-state actors are no less active: the American alt-right, for example, contributed to disinformation campaigns during the 2016 American presidential election, the 2017 French presidential election, and the 2017 German federal elections, at least. In March 2019, on the eve of European Parliament elections, the French newspaper *Le Monde* also revealed that American billionaires close to the right wing of the Republican Party were financing in Europe several “reinformation” websites and ad campaigns on digital platforms, spreading a radical and divisive ideology.[8]

In this context, and among the long list of electoral interference attempts in recent years, one case is especially important to study: the 2017 French presidential election. Not only did it concern the election of the head of a powerful state—the only nuclear power and permanent member of the United Nations (UN) Security Council in Europe after Brexit—but also, and above all, it failed. It failed in the sense that the result of the election did not coincide with the aim of the attackers.

> *“There was a coordinated attempt to undermine Macron’s candidacy, through a classic 3-dimension information operation”*

The French president is elected every five years, on a Sunday, by direct popular vote in two rounds (except if a candidate wins an absolute majority in the first round, which has never happened). In 2017, the first round took place on April 23, selecting the top two candidates out of eleven: Emmanuel Macron, thirty-nine, a centrist, liberal, and pro-European former economy minister who created his independent movement, En Marche! (Onward!), and Marine Le Pen, forty-eight, president of the far-right nationalist and populist National Front party, previously led by her father, Jean-Marie Le Pen. For the first time in the history of the

[7] David Spencer, “Fake news: How China is interfering in Taiwanese democracy and what to do about it,” *Taiwan News*, November 23, 2018, https://www.taiwannews.com.tw/en/news/3580979.

[8] Damien Leloup, “Des milliardaires américains financent discrètement des campagnes de désinformation en Europe,” *Le Monde*, March 7, 2019, https://www.lemonde.fr/pixels/article/2019/03/07/des-milliardaires-americains-financent-discretement-des-campagnes-de-desinformation-en-europe_5432486_4408996.html.

Fifth Republic, the current system of government established in 1958 by Charles de Gaulle, both final candidates were outside the bipolar, mainstream left-right party system. The second round between them took place on May 7.

2017 was a busy year for French democracy. As Laurent Fabius, president of the Constitutional Council, recalled, “For the first time since 1958, the presidential, legislative, and senatorial elections were held the same year.”[9] That coincidence did not go unnoticed: whoever was behind the attacks on the presidential election could have hoped to have a snowball effect on the other elections.

There was a coordinated attempt to undermine Macron’s candidacy, through a classic 3-dimension information operation: 1) a disinformation campaign consisting of rumors, fake news, and even forged documents; 2) a hack targeting the computers of his campaign staff; 3) a leak—15 GB of stolen data,[10] including 21,075 emails, released on Friday, May 5, 2017—just two days before the second and final round of the presidential election. This leak was promoted on Twitter by an army of trolls and fake accounts (bots) with the hashtag #MacronLeaks—even though none of the leaked documents actually came from Macron, only various sources related to him. The hashtag was thus spread first by those disseminating the leak, then by those criticizing it, appearing in almost half a million tweets in twenty-four hours, and so the attack is now remembered as “the Macron Leaks.” However, the leak itself was only the pinnacle of a coordinated operation that started months before, with a disinformation campaign and a hack. Therefore, we should rather speak of a “Macron Leaks” operation.

This operation could not sway French voters and change the result. Winning 66.1 percent of the vote, Macron defeated Le Pen. On Twitter, European Council President Donald Tusk congratulated Macron and the French people “for choosing Liberty, Equality, and Fraternity over tyranny of fake news,”[11] while Hillary Clinton wrote, “Victory for Macron, for France, the EU, & the world. Defeat to those interfering w/democracy.”[12] Macron, France’s youngest-ever president, had never held elected office before and was not a member of any political party. That was indeed a political “revolution”—the title of his campaign book. The legislative elections that took place in June gave him a clear majority, with his En Marche! movement becoming a political party, La République en marche (LREM), that dominates the parliament.

The “Macron Leaks” operation provoked a lot of interesting analysis, most of it contemporaneous, but some of it even quite far in advance, before it actually happened. As early as February 2, 2017, a famous information security researcher known only as “The Grugq” predicted, “Based on my analysis and what I’ve heard, I’m expecting leaks against Macron in the French election.”[13] He and others, like Nimmo, a leading expert on disinformation and how to fight it (“information defense”), produced invaluable analyses during the campaign and after the election. Many journalists, especially in France, also contributed greatly to our understanding of what was happening. The reader will find all these references in the footnotes. Two years later, this report does not pretend to reveal something new. Rather, its aim is to provide the most detailed single account to date of the “Macron Leaks” operation. With the benefit of hindsight, it will explore what happened, who (likely) orchestrated the affair, how it was successfully countered, and what lessons can be learned. In conclusion, it will also explain what France has accomplished since then and what is yet to be done.

[9] Conseil constitutionnel, *Annual Report* 2017, 5.

[10] Some sources say 15 GB, others 9.2 GB. Both are right: 9.2 GB is the size of the compressed archive that was initially uploaded, while 15 GB is the total size of its content once decompressed.

[11] Donald Tusk, “Congratulations @EmmanuelMacron. Congratulations to French people for choosing Liberty, Equality and Fraternity over tyranny of fake news.” Twitter Account, May 7, 2017, 11:40 a.m. https://twitter.com/eucopresident/status/861283142518353921.

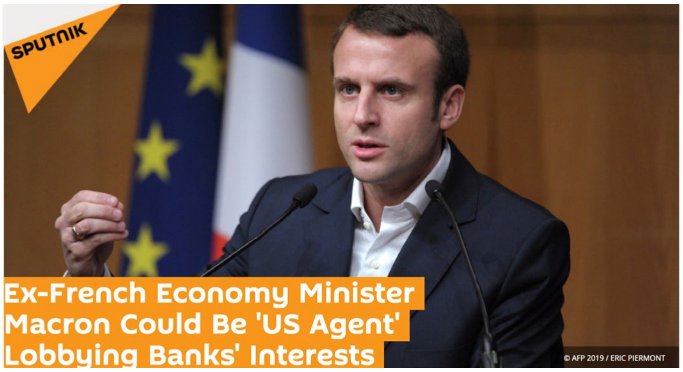
[12] Hillary Clinton, “Victory for Macron, for France, the EU, & the world. Defeat to those interfering w/democracy. (But the media says I can’t talk about that).” Twitter Account, May 7, 2017, 1:32 pm https://twitter.com/HillaryClinton/status/861317789537193988.

[13] Thaddeus Grugq, “Based on my analysis and what I’ve heard, I’m expecting leaks against Macron in the French election. More detailed explanation to come…” Twitter Account, February 2, 2017, 7:47 p.m. https://twitter.com/thegrugq/status/827362823500034049

I- WHAT HAPPENED

1. THE DISINFORMATION CAMPAIGN

The campaign against Macron began with rumors and insinuations, intensifying in January and February 2017. The timing was no coincidence: this was the exact moment when Macron, who had ranked third in most of the polls, became a front-runner because his most serious rival, François Fillon from the Republicans, was weakened by a political-financial scandal. As Macron overtook him in the polls and appeared to have a viable shot at the presidency, he became the target of more aggressive and more organized attacks from two sources: the Kremlin media (RT and Sputnik) and the American alt-right.



Ex-French Economy Minister Macron Could Be 'US Agent' Lobbying Banks' Interests

A Sputnik article presented Macron as a “US agent” backed by a “very wealthy gay lobby.” *Screenshot Source: https://sputniknews.com/analysis/201702041050340451-macron-us-agent-dhuicq*

a) By the Kremlin media

On February 3, 2017, in an article sensationally headlined, “Assange will throw oil on the fire of the presidential campaign in France,” the Russian newspaper *Izvestia* published an interview with Julian Assange in which the founder of WikiLeaks said, “We have interesting information about [Macron]. This data comes from the [hacked] personal correspondence of former US Secretary of State Hillary Clinton.”[14] Assange’s statement was all the more menacing given he had made similar ambiguous declarations before the 2016 American Democratic National Convention (DNC) leaks. His announcement was immediately spread by the French outlets of RT and Sputnik.[15] “RT France and Sputnik have been since the very beginning of our campaign the first source of fake news about our candidate and campaign,” Mounir Mahjoubi—then the digital manager of Macron’s campaign team —said later.[16] Here, it is worth recalling that Sputnik is the property of Rossiya Segodnya, which is the Russian government’s news agency and whose objective is to “secure the national interests of the Russian Federation in the informational sphere.”[17] Rossiya Segodnya and RT have the same chief editor, Margarita Simonyan, who once acknowledged that RT is needed “for about the same reason as why the country needs a Defense Ministry”. This quote, and others, seems to indicate, explains Nimmo, “that the station’s mission and philosophy are not journalistic but military, and it serves as an “information weapon””.[18] In February 2017, the Atlantic Council’s Digital Forensic Research Lab analyzed Sputnik France’s coverage and found a distinct bias against Macron.[19]

Only one day after Assange’s declaration, a Sputnik article presented Macron as a “US agent” backed by a “very wealthy gay lobby.”[20] The “gay” card was nothing new: it

[14] “Ассанж подольет масла в огонь предвыборной кампании Франции,” Известия, February 3, 2017, https://iz.ru/news/661960.

[15] See “Assange: WikiLeaks a trouvé des informations sur Macron dans des emails de Clinton,” RT France, February 3, 2017, https://francais.rt.com/france/33403-wikileaks-macron-clinton-email-assange and “Assange: des révélations sur Macron dans les mails de Clinton,” Sputnik, February 3, 2017, https://fr.sputniknews.com/international/201702031029930563-wikileaks-revelations-macron/.

[16] Christopher Dickey, “Fighting Back Against Putin’s Hackers,” *The Daily Beast*, April 25, 2017, https://www.thedailybeast.com/fighting-back-against-putins-hackers.

[17] Ben Nimmo, “Thread on Sputnik, and some of the ways it fulfils its official task of ‘securing the national interests of the Russian Federation in the information sphere.’ Yep, that’s a quote.” Twitter Account, 1 July 2018, https://threadreaderapp.com/thread/1009776438298411010.html

[18] Ben Nimmo, “Question That: RT’s Military Mission Assessing Russia Today’s role as an “information weapon””, *Atlantic Council’s Digital Forensic Research Lab, Medium.com*, 8 January 2018. https://medium.com/dfrlab/question-that-rts-military-mission-4c4bd9f72c88

[19] Ben Nimmo, “Frankly Unfair? Fact checking Sputnik France’s claim that it is reporting the French election fairly,” *Atlantic Council’s Digital Forensic Research Lab, Medium.com*, February 11, 2017, https://medium.com/dfrlab/frankly-unfair-3a43f4347dfe.

[20] “Ex-French Economy Minister Macron Could Be ‘US Agent’ Lobbying Banks’ Interests,” Sputnik, February 4, 2017, https://sputniknews.com/analysis/201702041050340451-macron-us-agent-dhuicq//.

In early February, Fillon’s popularity was damaged by the so-called “Fillon affair,” or “Penelopegate” named for his wife. *Photo credit: Wikimedia Commons https://fr.wikipedia.org/wiki/Fichier:2016-10-19_16-21-56_fillon-belfort.jpg*

first appeared in the summer of 2014 when Macron was nominated as minister of the economy. In May 2016 it spread across Twitter and has been regularly used by his political opponents ever since.[21] At first, Macron ignored the comments but, at the beginning of his campaign, in early November 2016, he decided to confront them.[22] However, that was not enough: the rumors became so insistent that on February 7, only three days after the Sputnik article, Macron humorously denied that he was having an extramarital gay relationship.[23]

When confronted with this specific article, Rossiya Segodnya (Sputnik) and RT Editor-in-Chief Margarita Simonyan said that this information, like everything her outlets publish on France, was drawn directly from French news sources, claiming, “We have never published anything that has not already been published by the French media.”[24] Knowing that they are under scrutiny, RT and Sputnik proceed cautiously and indirectly, preferring to quote others. They find the right people, make them talk about Macron, and then pick and choose the juiciest quotations.

In this instance, they had interviewed Nicolas Dhuicq, a pro-Russian, right-wing French member of parliament. Just a few weeks before, Dhuicq and his friend Thierry Mariani, another member of parliament (MP), were in Damascus. Since 2015, the two members of the French-Russian Dialogue, a pro-Russia lobby, have supported Moscow’s military intervention in Syria, against the official position of the French government. They visited Syria and met with President Bashar al-Assad several times. At the time, both were with Fillon’s Republicans. Since then, Dhuicq has joined Debout la France, a small nationalist, Euroskeptic party, and Mariani—who was also serving on the “ethics committee” of RT France—joined Marine Le Pen’s renamed party, the National Rally (formerly the National Front).

This is how RT and Sputnik operate. Rarely do they create strictly fake content—and this is another reason to reject the term “fake news” and to prefer the broader term “information manipulation” (see below). Most of the time, they rather express a strong bias, leaving important information out and/or hiding behind the quotations of others, often very partisan people. Quotations provide an illusion of truth and journalistic integrity.

Sputnik used the same method and the same defense a few days later, on February 9, when the outlet published an article claiming that French journalists in Moscow had been seen wearing En Marche! T-shirts[25]—fueling rumors that the mainstream media were biased in Macron’s favor. These allegations were proved false: none of the three correspondents present at the En Marche! meeting was wearing a partisan T-shirt. When confronted on this fact, Simonyan used the same defense as before: the article was “based on quotations from the representative of the Republicans in Moscow.”[26] Again, Sputnik chose its interviewee well: Alexis Tarrade, the representative of a political party

[21] Quentin Girard, “Macron gay? La fabrique d’une rumeur,” *Libération*, February 7, 2017, https://www.liberation.fr/france/2017/02/07/macron-gay-la-fabrique-d-une-rumeur_1546935.

[22] Bruno Rieth, “Rumeur sur sa ‘double vie’ : Emmanuel Macron sort du silence,” *Marianne*, November 3, 2016, https://www.marianne.net/politique/rumeur-sur-sa-double-vie-emmanuel-macron-sort-du-silence.

[23] Nathalie Raulin, “Macron gay ? L’intéressé se marre,” *Libération*, February 7, 2017, https://www.liberation.fr/france/2017/02/07/macron-gay-l-interesse-se-marre_1547015.

[24] Margarita Simonyan, interviewed in the documentary *La guerre de l’info: au cœur de la machine russe*, directed by Paul Moreira, 2017.

[25] “Quand ‘les journalistes français portent des T-shirts En Marche!’ en Russie,” Sputnik France, February 9, 2017, https://fr.sputniknews.com/international/201702091030021060-communique-lr-russie/.

[26] Benjamin Quenelle, “Le succès de Macron ou les limites de l’influence des médias russes,” *LesEchos.fr*, April 25, 2017, https://www.lesechos.fr/2017/04/le-succes-de-macron-ou-les-limites-de-linfluence-des-medias-russes-166010#xtor=RSS-37.

rival to Macron's. Sputnik did use quotation marks, but it did not check the claim, nor did it interview a representative from En Marche! or a French journalist among those present that day. Sputnik just took the claim at face value, and to illustrate this point it even posted a photo of a group of people wearing En Marche! T-shirts. However, these people happened to be the En Marche! team in Moscow, not French press correspondents in Moscow. As Nimmo summed up, "Sputnik's piece was therefore wholly unbalanced and rested on an unsubstantiated accusation by one of Macron's political opponents, and a photo which was taken out of context, if not actively misrepresented."[27]

In early February, Fillon's popularity was damaged by the so-called "Fillon affair," or "Penelopegate" named for his wife, who was suspected of having received as much as €813,440 as a parliamentary assistant to her husband for very little or no actual work, and then €100,000 as a literary adviser to the *Revue des deux Mondes*. The affair proved to be serious: in March 2017, the national financial prosecutor placed him under formal investigation for "aggravated fraud, forgery, falsification of records," and influence-peddling. Fillon was initially the favorite in the polls: this affair ruined his chance to win the presidency. A few months earlier, Macron's other main rival, Marine Le Pen, was ordered by the EU anti-corruption body to repay over €300,000 of misspent EU funds. She was also under investigation for posting three graphic images from the Islamic State on Twitter, including the beheading of an American journalist—another affair over which the European Parliament lifted her immunity in early March 2017. Therefore, at this stage of the presidential campaign, there were indeed some real "affairs" going on. However, Sputnik preferred to focus on an invented "Macron affair": "It must be said here that there is a Macron 'affair,'" explained Jacques Sapir, a regular Sputnik and RT commentator—even though this time Sputnik took the precaution of adding, "The opinions expressed in this content are the sole responsibility of the author."[28]

Overall, after a rigorous analysis of Sputnik's coverage of the presidential campaign, Nimmo concluded, "Repeatedly, Sputnik France has focused on accusations of corruption and media bias towards Macron; it has defended Le Pen and amplified her party. It has published unbalanced reports, giving one side of the story and leaving the other silent."[29]

b) By the American alt-right

The Kremlin was not the only player involved. Some attacks against Macron came from the West. Journalist Josh Harkinson called these actors "Marine Le Pen's 'Foreign Legion' of American Alt-Right Trolls."[30] These "trolls" were active on Reddit, 4chan's political board, and other similar forums. "Using fake French identities and sock puppet social-media accounts, they've hijacked Twitter hashtags, social-media posts, and comments sections on news sites with memes portraying Macron as a stooge of Jewish financiers who will sell out the working class and capitulate to Muslim terrorists," Harkinson wrote.[31] Some attacks were political—calling Macron an aristocrat who despises the common man, a rich banker, a globalist puppet, a supporter of Islamic extremism and uncontrolled immigration, and alleging that a vote for him was a vote for another five years of President Francois Hollande (the unpopular Socialist incumbent president). Others were personal, including salacious remarks about the age difference between him and his wife, rumors that he was having an affair with his stepdaughter, and speculation over his sexuality.

One notable example of disinformation based on the "Islam" narrative was a March 2 article designed to appear as if it came from the Belgian newspaper *Le Soir*, headlined "Emmanuel Macron, Saudi Arabia's preferred candidate in the French presidential election." The article appeared on a cloned website, imitating almost perfectly the design and layout of *Le Soir*, but using a different URL, lesoir.info instead of lesoir.be. It was circulated by Marion Maréchal-Le Pen, a parliamentarian and niece of Marine Le Pen, indignantly asking: "30% of the Macron campaign financed by Saudi Arabia? We demand transparency!". Her tweet was shared more than two hundred times in half an hour, including by presidential candidates Le Pen (her aunt) and Fillon,

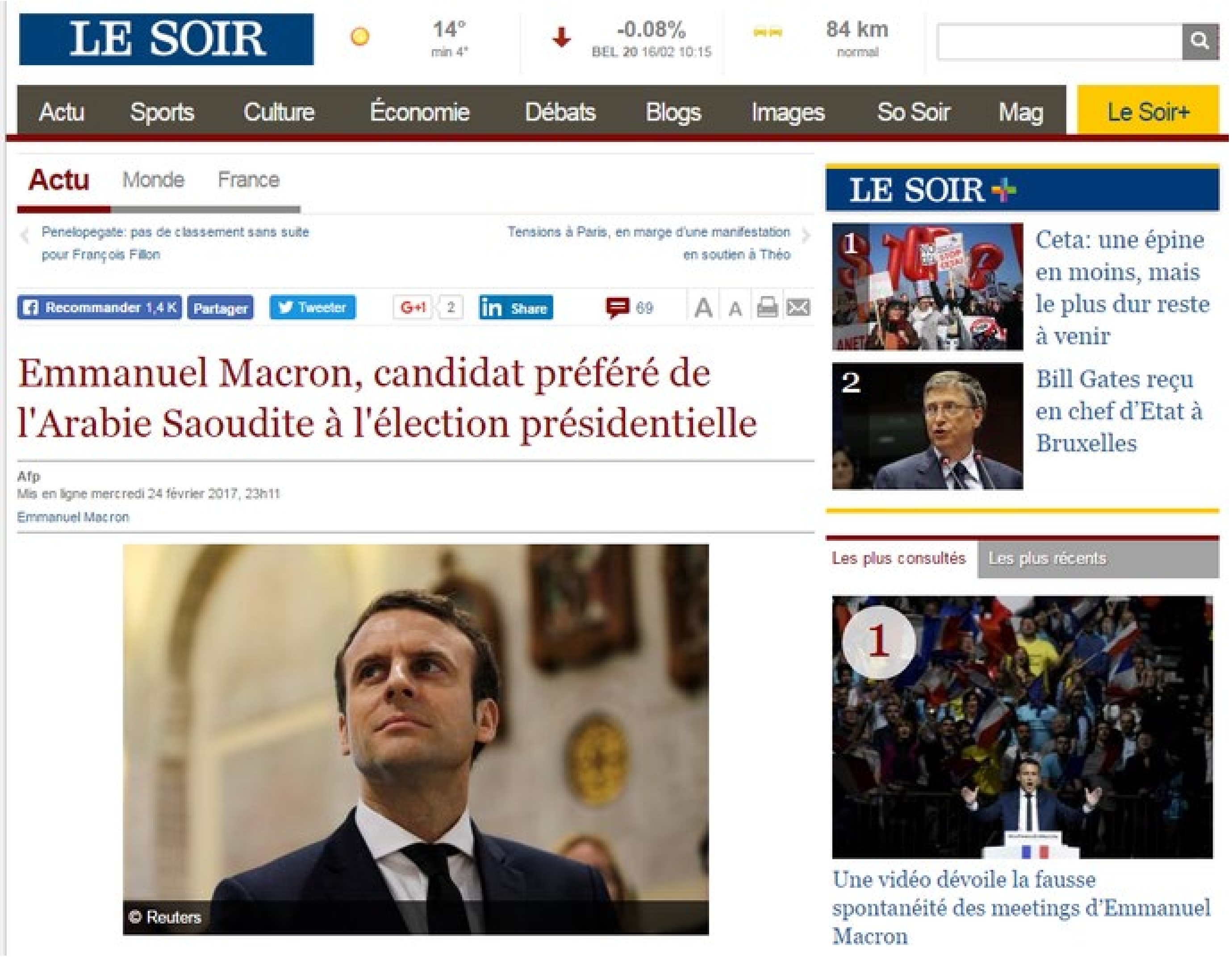
[27] Nimmo, "Frankly Unfair?".

[28] Jacques Sapir, "L'essentiel, l'accessoire et l'affaire Fillon," Sputnik France, February 7, 2017, https://fr.sputniknews.com/points_de_vue/201702071029952981-france-fillon-chomage/.

[29] Nimmo, "Frankly Unfair?" See also Ben Nimmo, "The French election through Kremlin eyes," DFRLab Medium.com, April 20, 2017, https://medium.com/dfrlab/the-french-election-through-kremlin-eyes-5d85e0846c50.

[30] Josh Harkinson, "Inside Marine Le Pen's 'Foreign Legion' of American Alt-Right Trolls," *Mother Jones*, May 3, 2017, https://www.motherjones.com/politics/2017/05/marine-le-pen-alt-right-american-trolls/.

[31] *Ibid.*



Penelopegate: pas de classement sans suite pour François Fillon

Tensions à Paris, en marge d'une manifestation en soutien à Théo

Emmanuel Macron, candidat préféré de l'Arabie Saoudite à l'élection présidentielle

Afp
Mis en ligne mercredi 24 février 2017, 23h11
Emmanuel Macron

Ceta: une épine en moins, mais le plus dur reste à venir

Bill Gates reçu en chef d'Etat à Bruxelles

Une vidéo dévoile la fausse spontanéité des meetings d'Emmanuel Macron

One notable example of disinformation based on the “Islam” narrative was a March 2 article designed to appear as if it came from the Belgian newspaper *Le Soir*, headlined “Emmanuel Macron, Saudi Arabia’s preferred candidate in the French presidential election.” *Source: https://www.lemonde.fr/les-decodeurs/article/2017/03/02/macron-finance-par-l-arabie-saoudite-une-intox-massivement-relayee-par-l-extreme-droite_5088356_4355770.html*

before she deleted it.[32]

In January 2017, Buzzfeed News infiltrated a Discord-based gaming community private chatroom called “The Great Liberation of France,” “focused on social media and memetic actions in order to help Marine Le Pen’s campaign.”[33] This rare access gave a glimpse at their strategy and tactics. Their main activity was to help users create fake Facebook and Twitter accounts. At the time Buzzfeed entered the chatroom, Le Pen’s rival, and therefore the main target of these alt-right trolls, was Fillon, the then-front-runner for the presidency. Pieces of advice shared in the chatroom included to “make leftist accounts and attack the shit out of him mercilessly” and “bring up that 10 years ago Fillon was for gay marriage and was pro-choice.” One of their leaders, going by the name @trumpwin2016, gave more general instructions, like creating fake accounts that are “ideally young, cute girl, gay, Jew, basically anyone who isn’t supposed to be pro-FN [Front National].” He adds, “It needs to be done by our French and Francophone users so it looks authentic, not just like Americans trying to

[32] “Was Macron’s campaign for the French presidency financed by Saudi Arabia?”, *Crosscheck*, March 2, 2017.

[33] Ryan Broderick, “Trump Supporters Online Are Pretending To Be French To Manipulate France’s Election,” *BuzzFeed News*, January 24, 2017. The quotes in the next two paragraphs come from this article, https://www.buzzfeednews.com/article/ryanhatesthis/inside-the-private-chat-rooms-trump-supporters-are-using-to.

take the Trump Train to Europe."

This community shared a Google document titled "MEGA GENERAL," MEGA for "Make Everything Great Again," which starts with a clear ambition: "We have won our first major battle, now we have to rescue the rest of the world." In order to do so, the document lists targets (Austrian election, Italian referendum, Dutch election, French election, and German election), acknowledges that "we need as much national operatives as possible," and gives instructions: if you want the American alt-right to help promote your nationalist candidate in your local election, you have to "provide reconnaissance" first because they "don't know shit about your internet segment." They need to know what the popular vectors are in your country, digital platforms, journalists, etc. They also need info on the "dark past" of your candidate's rivals, divisive issues in your country, etc. And, to those in the United States or elsewhere but outside the target state willing to help, they caution against failing "to disguise yourself as a national." So they need to really "listen to what nationals say" and should not post content "in a foreign language without checking with a national operative. Better yet, create everything in English, post in the thread and ask a national to translate it." As a matter of fact, the American community of "The Great Liberation of France" worked regularly with their French counterparts, a far-right Discord chatroom called "La Taverne des patriotes."

"These communities are a venue where American alt-right, French far-right, and other pro-Kremlin actors can meet."

Who were the people in "The Great Liberation of France" chatroom? Most of them were 4chan users. Not only American alt-right and French far-right but also more generally the international alt-right. One of the users interviewed by Buzzfeed also mentions "Russian neo-fascists like Alexander Dugin": "The shared agenda is to get far right, pro-Russian politicians elected worldwide." However, at the end of April 2017, on the eve of the first round, "The Great Liberation of France" had no more than forty users, who posted a few messages over a period of weeks. Most of the others apparently moved to another Discord chatroom called "Centipede Central."[34]

"The shared agenda is to get far right, pro-Russian politicians elected worldwide"

Another interesting place is the pro-Trump subreddit "The_Donald." On May 6, at the strategic moment between the leak (the day before) and the final vote (the day after), guidelines for the French willing to "save [their] country" were posted.[35] On method, "First priority is to get Macron voters to stay home. There's already a hashtag going on the left to not vote - fuel this by dissuading your friends from voting. They have to feel Macron is a bad choice. You do this publicly on your social media accounts (we have some memes you can use below). Use the known hashtag #SansMoiLe7mai - pretend you won't vote (you will)." Another piece of advice is to "not blatantly yell at people to vote for Marine. We're too close to the election for it to be about partisanship - it's much easier to discourage people from voting than to overcome decades of media slander against Marine." As for content, the recommendation is to focus on five narratives, "5 things Macron doesn't want the French people to know":

> "1. He plans to re-write history with Muslim countries to teach French children Islam was always part of France. This is cultural genocide.[36]
>
> 2. He has secret accounts in the Cayman Islands.[37]
>
> 3. He and his team have been rigging elections.[38]
>
> 4. As always, the rules don't apply to the elite - his team has been ordering illegal drugs including

[34] William Audureau and Corentin Lamy, "Sur Internet, l'extrême droite anglophone tente péniblement de s'organiser pour nuire à Macron," *Le Monde*, April 25, 2017.

[35] The_Donald, "FRENCH MEDIA IS SHUT DOWN. WE'RE NOT. HERE ARE 5 THINGS MACRON DOES NOT WANT THE FRENCH PEOPLE TO KNOW." Reddit, May 6, 2017, https://i.reddit.com/r/The_Donald/comments/69nn5j/french_media_is_shut_down_were_not_here_are_5/?limit=500

[36] Diversity Macht Frei, "Macron Leaks contain secret plans for the islamisation of France and Europe". Diversity Macht Frei, Blogspot, May 6, 2017, https://diversitymachtfrei.blogspot.com/2017/05/macron-leaks-contain-secret-plans-for.html

[37] June, "BREAKING: MACRON BUSTED! Lied About Tax Evasion? – 4Chan /pol/ Posts Images from Macron's Off-Shore Bank Account!" The Gateway Pundit, May 4, 2017, https://www.thegatewaypundit.com/2017/05/breaking-macron-busted-lied-tax-evasion-4chan-pol-posts-images-macrons-off-shore-bank-account/

[38] The_Donald, "CONFIRMED: FRENCH ELECTION RIGGED!" Reddit, May 5, 2017, https://www.reddit.com/r/The_Donald/comments/69iqef/confirmed_french_election_rigged/

All this happened during the televised debate and, just before 11:00 p.m., Le Pen herself said on air, “I hope we will not find out, Mr. Macron, that you have an offshore account in the Bahamas.” *Photo Credit: © Copyright AFP Source: Macron Le Pen debate - REUTERS/Eric Feferberg/Pool*

> cocaine to the French parliament, further adding to the strong suspicion of Macron being the latest puppet to the banker elites that control French government.[39]
>
> 5. The French media has been deleting right-wing content and Facebook has been colluding to delete right-wing commentators for the past 72 hours.”[40]

Such chatrooms (there are others) very professionally supply the means and methods of warfare. They are not interesting for themselves, as these pages are ephemeral and their users quite mobile. They seek to protect their confidentiality and are aware of the attention they attract not only from intelligence services but also from journalists, who sometimes manage to infiltrate and expose them. What is interesting is the fact that such communities, on Discord, Reddit or elsewhere, are intersections among several communities of interest. They are a venue where American alt-right, French far-right, and other pro-Kremlin actors can meet. And that tells us something on attribution, as these communities provide an alternative explanation for who is “behind” attacks like the “Macron Leaks” operation. It does not have to be someone in particular—it can be a common and decentralized effort by like-minded people, following user manuals like the ones above. This obviously makes attribution more difficult, but it is probably closer to reality.

2. THE APERITIF: #MACRONGATE

Last but not least came the “#MacronGate” rumor. Two hours before the final televised debate between Macron and Le Pen, on Wednesday, May 3, at 7:00 p.m.,[41] a user with a Latvian IP address posted two fake documents on 4chan. The documents suggested that Macron had a company registered in Nevis, a small Caribbean island, and a secret offshore bank account at the First Caribbean Bank, based in the Cayman Islands. Again, the rumor itself was not entirely new. Macron himself had seen it coming. More than two weeks earlier on TV he warned that this type of rumor was likely to appear: “This week, you will hear ‘Mr. Macron has a hidden account in a tax haven, he has money hidden at this or that place.’ This is totally false, I always paid all my taxes in France and I always had my accounts in France.”[42] What was new this time, however, was the release of two documents supposedly proving this

[39] email@buckled.com, screen capture of message to fm.alaintourret@gmail.com, http://i.imgur.com/lQQXbrG.jpg

[40] Jim Hoft, “Facebook Suspends 30,000 French Accounts 10 days Before Election in Attempt to Censor Le Pen Supporters”. The Gateway Pundit, April 14, 2017, https://www.thegatewaypundit.com/2017/04/facebook-suspends-30000-french-accounts-10-days-election-attempt-censor-le-pen-supporters/

[41] All timestamps in this report are presented in Central European Summer Time.

[42] Emmanuel Macron interviewed by Jean-Jacques Bourdon on BFM-TV, April 17, 2017.

In one instance, the Macron campaign team received an email apparently from Mahjoubi–the email address was almost identical to Mahjoubi’s, apart from one missing letter. *Photo Credit REUTERS/Charles Platiau*

rumor.

The user who posted the two documents on 4chan did it purposefully on the evening on the final televised debate to attract more attention, and even suggested a French hashtag: “If we can get #MacronCacheCash trending in France for the debates tonight, it might discourage French voters from voting Macron”[43].

Then the rumor spread on Twitter. The 4chan link was first posted by Nathan Damigo, founder of the American neo-Nazi and white-supremacist group Identity Evropa, and was further circulated by William Craddick, founder of Disobedient Media and notorious for his contribution to the Pizzagate conspiracy theory that targeted the US Democratic Party during the 2016 American presidential campaign. The first real amplifier was Jack Posobiec—an American alt-right and pro-Trump activist with 111,000 followers at the time: his tweet was retweeted almost 3,000 times. Only after 10:00 p.m. did the rumor begin to spread in French, mostly through far-right accounts using the #MacronCacheCash hashtag. The first tweets in French seemed to have been automatically translated from English.[44]

All this happened *during* the televised debate and, just before 11:00 p.m., Le Pen herself said on air, “I hope we will not find out, Mr. Macron, that you have an offshore account in the Bahamas.” The following morning, Macron’s campaign team denounced a “campaign of digital disinformation on a scale and with a level of professionalism that is troubling.”[45] Mahjoubi considered Le Pen’s insinuations as “an admission”: “She referred to a rumor that had not even started.”[46] Macron himself believed she did not work alone: this “fake news” was premeditated “with her allies. … There are people who spoke to each other and organized themselves.”[47] The rumor was quickly debunked as several researchers and reliable media sources decisively proved these documents to be fabricated.[48]

However, this was only the beginning. The same user with the Latvian IP address who posted the fake documents on Wednesday announced on Friday morning that more were coming, promising, “We will soon have swiftnet logs going back months and will eventually decode Macron’s web of corruption.”[49] Those responsible for #MacronGate thereby provided evidence that they were the same people responsible for the #MacronLeaks that were released later that day.

3. THE HACK

The leak of stolen data was logically preceded by a hack. It started with a series of phishing attacks. Macron’s team confirmed that they had been targeted since December 2016.[50] Knowing that Macron’s team used Microsoft OneDrive for emails and storage, the attackers sent staff members official-looking emails

[43] Crosscheck, “Did Emmanuel Macron open an offshore account ?”, Crosscheck, 5 May, 2017. https://crosscheck.firstdraftnews.org/checked-french/emmanuel-macron-open-offshore-account/

[44] As noted by Stephanie Lamy, who was one of the first to analyze the spread on Twitter: https://twitter.com/WCM_JustSocial/status/859930146102489089.

[45] Renaud Lecadre, Dominique Albertini, and Amaelle Guiton, “ ‘Compte aux Bahamas’: Macron ciblé par le poison de la rumeur,” *Libération*, May 4, 2017, https://www.liberation.fr/politiques/2017/05/04/compte-aux-bahamas-macron-cible-par-le-poison-de-la-rumeur_1567384.

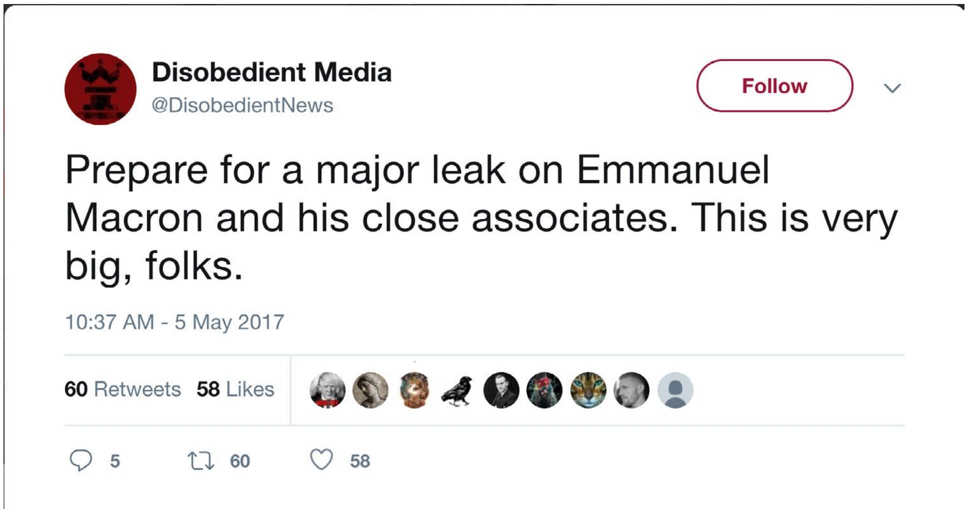
[46] Morgane Tual, “Macron et l’évasion fiscale: itinéraire d’une rumeur, de 4chan aux plateaux télé,” *Le Monde*, May 4, 2017, https://www.lemonde.fr/pixels/article/2017/05/04/macron-et-l-evasion-fiscale-itineraire-d-une-rumeur-de-4chan-aux-plateaux-tele_5122473_4408996.html.

[47] Emmanuel Macron on France Inter Radio, May 4, 2017.

[48] “How we debunked rumours that Macron has an offshore account,” France 24–The Observers, May 5, 2017. See also Lecadre, Albertini, and Guiton, “ ‘Compte aux Bahamas.’ ”

[49] Chris Doman, “MacronLeaks–A Timeline of Events,” AlienVault, May 6, 2017, https://www.alienvault.com/blogs/labs-research/macronleaks-a-timeline-of-events.

[50] Dickey, “Fighting Back Against Putin’s Hackers.”


Disobedient Media
@DisobedientNews

Prepare for a major leak on Emmanuel Macron and his close associates. This is very big, folks.

10:37 AM - 5 May 2017

60 Retweets 58 Likes

Disobedient Media, “Prepare for a major leak on Emmanuel Macron and his close associates. This is very big, folks.” Twitter Account, May 5, 2017, 7:37 p.m. (CEST) *Photo credit: Twitter*

asking them to click on links with seemingly cloud data storage or webmail domains (onedrive-en-marche.fr, mail-en-marche.fr, portal-office.fr, and accounts-office.fr).[51] “If you speed read the URL, you can’t make the distinction” Mahjoubi said, while the decoy sign-in page was “pixel perfect,”[52] convincing enough for someone to enter their login credentials.

Other techniques included tabnabbing[53] or email spoofing. In one instance, the Macron campaign team received an email apparently from Mahjoubi—the email address was almost identical to Mahjoubi’s, apart from one missing letter (mounir.mahjobi@... instead of mounir.mahjoubi@...). Titled “Recommendations against cyberattacks,” it read as follows: “Due to numerous cyberattack attempts, please be vigilant. Our experts have implemented detailed recommendations against piracy. You will find the document attached.”[54] In another instance, campaign staffers received an email apparently from the head of press relations providing “some recommendations when [talking] to the press” and inviting them to “download the attached file containing talking points.”[55]

In total, the professional and personal email accounts of at least five of Macron’s close colleagues were hacked: the Gmail accounts of Quentin Lafay (speechwriter), Anne-Christine Lang (Socialist Party MP for the department of Paris), Alain Tourret (Radical Party of the Left and Socialist Party MP for the department of Calvados), Pierre Person (co-founder and president of “The Young With Macron” movement), along with his Google Drive, and the en-marche.fr account of Cédric O (En Marche! treasurer).[56] The stolen emails range from March 20, 2009, to April 24, 2017,[57] indicating that at least one of the successful attacks had occurred that day.

4. THE LEAK

Leaking as an informational technique has been used by

[51] Amaelle Guiton, “En marche, cible des hackers de Fancy Bear?” *Libération*, April 24, 2017.

[52] Dickey, “Fighting Back Against Putin’s Hackers.”

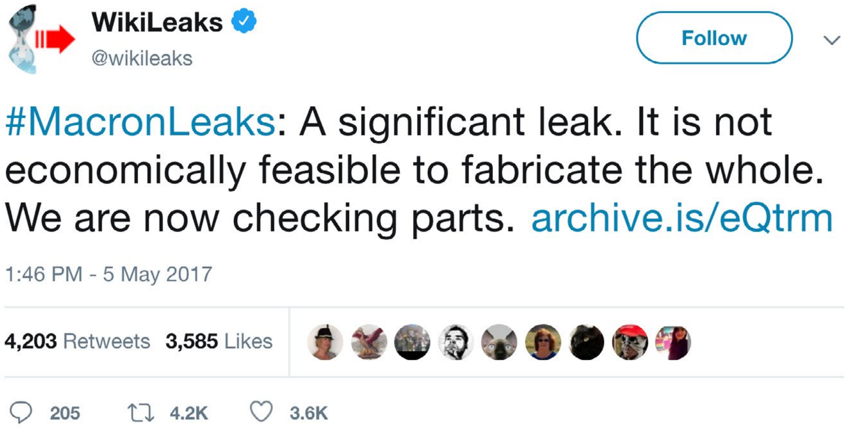
[53] “The target gets an email supposedly coming from a website he might be interested in–maybe from a conference he is likely to visit or a news site he has subscribed to. The email has a link to a URL that looks very legitimate. When the target reads his email and clicks on the link, it will open in a new tab. This new tab will show the legitimate website of a conference or news provider after being redirected from a site under the attackers’ control. The target is likely to spend some time browsing this legitimate site. Distracted, he probably did not notice that just before the redirection, a simple script was run, changing the original webmail tab to a phishing site. When the target has finished reading the news article or conference information on the legitimate site, he returns to the tab of his webmail. He is informed that his session has expired and the site needs his credentials again. He is then likely to reenter his password and give his credentials away to the attackers.” (Feike Hacquebord, *Two Years of Pawn Storm: Examining an Increasingly Relevant Threat, A Trend Micro Research Paper*, April 25, 2017, 14 https://tinyurl.com/yy4hsym8). Mahjoubi acknowledged that the En Marche! movement “has been hit by it.” (Dickey, “Fighting Back Against Putin’s Hackers.”)

[54] Mahjoubi, interviewed in the documentary *La guerre de l’info*.

[55] Mahjoubi, interviewed in Antoine Bayet, “Macronleaks: le responsable de la campagne numérique d’En marche! accuse les ‘supports’ du Front national,” France Info, May 8, 2017.

[56] Frédéric Pierron, “MacronLeaks: 5 victimes et des failles de sécurité,” *fredericpierron.com blog*, May 11, 2017.

[57] The “Macron Campaign Emails” WikiLeaks archive, https://wikileaks.org/macron-emails.



WikiLeaks @wikileaks

#MacronLeaks: A significant leak. It is not economically feasible to fabricate the whole. We are now checking parts. archive.is/eQtrm

1:46 PM - 5 May 2017

4,203 Retweets 3,585 Likes

205 4.2K 3.6K

It was WikiLeaks that internationalized the spread, at 9:31 p.m., by tweeting: "#MacronLeaks: A significant leak. It is not economically feasible to fabricate the whole. We are now checking parts." *Photo credit: Twitter:*

genuine whistleblowers as well as by ill-intentioned foreign powers–the obvious precedent for the latter being the 2016 DNC email leak during the US presidential campaign. Leaks are enticing because they "appear to provide an unfiltered peek at people speaking privately. Like an intercepted conversation, they [make us] feel closer to the 'truth,' and may indeed reveal unscripted truths about people and institutions."[58]

The hackers waited until the very last moment to leak the documents: Friday, May 5, 2017, hours before official campaigning stopped for the period of "election silence," a forty-four-hour media blackout ahead of the closing of the polls. Between midnight on Friday and 8:00 p.m. on Sunday, when the last polls close, candidates are prohibited by law from making public statements or giving interviews. The leak was so timed to leave Macron and his party powerless to defend themselves, to block the mainstream media from analyzing the documents and their release, and to make social media, especially Twitter, "the primary space where the content could be discussed."[59] In other words, "Twitter was used as a communication back-channel to talk about an event where conventional media sources were prohibited from participating."[60]

Craddick (Disobedient Media) was the first to act (or react). At 7:37 p.m., he tweeted, "Prepare for a major leak on Emmanuel Macron and his close associates. This is very big, folks."[61] The fact itself that Craddick knew about the leak before it was shared is sufficient to conclude, as analyst Kris Shaffer does, that "Disobedient Media is a source worth a closer investigation."[62]

"It was WikiLeaks that internationalized the spread"

The files were initially posted on Archive.org, an online library site, supposedly in the morning[63] (the time of first release on the website cannot be determined, as these original threads have since been deleted). At 7:59 p.m., the links to the threads were posted on PasteBin, a file-sharing site, under the name "EMLEAKS." At 8:35 p.m., they were shared on 4chan. Then came their appearance on Twitter: Craddick was again the first to share the link to the PasteBin dump at 8:47 p.m., quickly followed by Jack Posobiec at 8:49 p.m., who provided a link to the 4chan thread with, for the first time, the hashtag #MacronLeaks.[64] Contrary to

[58] Adam Hulcoop *et al.*, "Tainted Leaks: Disinformation and Phishing With a Russian Nexus," *The Citizen Lab*, May 25, 2017, https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/.

[59] Wasim Ahmed and Joseph Downing, "Campaign leaks and the far-right: Who influenced #Macronleaks on Twitter?" *LSE European Politics and Policy (EUROPP) blog*, June 12, 2017, https://blogs.lse.ac.uk/europpblog/2017/06/12/who-influenced-macronleaks-on-twitter/.

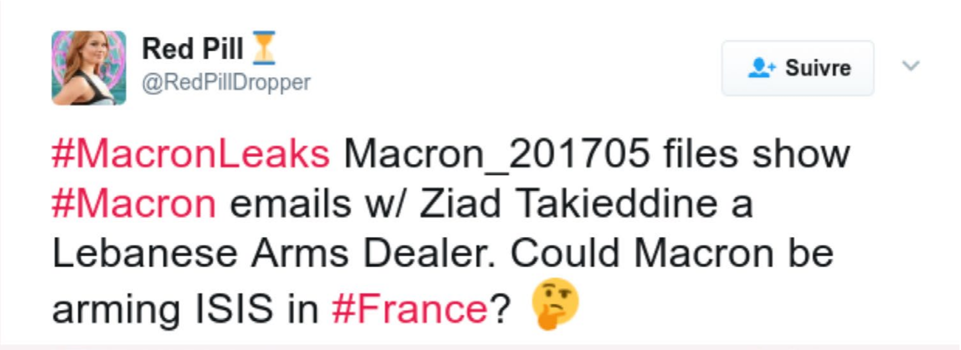
[60] *Ibid*.

[61] Disobedient Media, "Prepare for a major leak on Emmanuel Macron and his close associates. This is very big, folks." Twitter Account, May 5, 2017, 10:37 am https://twitter.com/DisobedientNews/status/860549138139795456

[62] Kris Shaffer, "#MacronLeaks–how disinformation spreads," *pushpullfork.com*, May 19, 2017.

[63] Telefonica, *En Marche: MacronLeaks, Cybersecurity Shot*, May 8, 2017, 3.

[64] Jack Posobiec, "Massive doc dump at/pol/ "Correspondence, documents, and photos from Macron and his team'" Twitter Account,



Red Pill ⏳
@RedPillDropper

#MacronLeaks Macron_201705 files show #Macron emails w/ Ziad Takieddine a Lebanese Arms Dealer. Could Macron be arming ISIS in #France? 🤔

This unrelated folder, with an intentionally misleading title, was enough to trigger fanciful rumors, such as one claiming that, through Takkiedine, Macron was actually working with ISIS. *Photo credit: Twitter*

what would later become a widespread misconception, Posobiec was not the first to tweet, Craddick was. However, Posobiec was the first to use the hashtag that would lend its name to the entire operation, hence the confusion. Posobiec’s tweet and hashtag was retweeted eighty-seven times within five minutes. He later said he had been alerted to the incoming dump by the user with a Latvian IP address who had posted the #MacronGate fake documents two days prior: “The same poster of the financial documents said to stay tuned tomorrow for a bigger story–so I pretty much spent the next 24 hours hitting refresh on the site.”[65]

So far, this conversation was exclusively Anglophone. This makes it clear that the hashtag #MacronLeaks was launched and spread in the United States, by the American alt-right. It was WikiLeaks that internationalized the spread, at 9:31 p.m., by tweeting: “#MacronLeaks: A significant leak. It is not economically feasible to fabricate the whole. We are now checking parts,” with a link to the files on PasteBin. Only then came the first French amplifiers, who happened to be Le Pen supporters. Only two of them made it into the ten most-popular tweets, though: Florian Philippot, vice president of the National Front Party (his 11:40 p.m. tweet was, until the following morning, “the tweet which received the most replies”[66]) and a National Front activist calling himself Samuel (account @Messsmer), one of the leaders of the self-proclaimed “*patriosphère*” (patriot sphere) who had been an active contributor to the online campaign against Macron since early 2017 (with #DemasquonsMacron, #LePionMacron, #LeVraiMacron, etc.).[67] Another French catalyst account was @KimJongUnique, “one of the most influential of the Russosphere [the French-speaking, pro-Russian online community].”[68]

A study of the French pro-Russian Twittersphere shows that it is “not homogeneous, either based on the profile of individuals which compose it or based on their political leanings. On the contrary, it is a very diverse galaxy which could largely exist without any kind of action from Russia. We can see however that the ‘central’ accounts, being politicians or Russian media, are important to create connections and coherence within the galaxy.”[69] In their database of 23,036 accounts involved in the #MacronLeaks Twitter conversation, the authors found that only 1.5 percent “can be considered as potential active supporters of Russian informational activities. Yet … if they are not numerous, these accounts made ‘a lot of noise,’ and took an important part in the virality of the keyword. … [They] proved to be approximately twice as active as the others.”[70]

Overall, the hashtag “#MacronLeaks reached forty-seven thousand tweets in just three and a half hours after the initial tweet.”[71] On Friday night, the Twitter

May 5, 2017 8:49 a.m. https://twitter.com/JackPosobiec/status/860567072010620929

[65] Jack Posobiec, interviewed by Megha Mohan, “The Anatomy of a Hack,” *BBC Trending*, May 9, 2017.

[66] *Ibid*.

[67] Jacques Pezet, “Comment les trolls ‘patriotes’ ont lancé l’attaque #LeVraiMacron,” *Libération*, February 11, 2017, https://tinyurl.com/y5rdpelw ; Yoann Saby, “Je suis Samuel, je suis militant. Je suis là pour la grandeur de la France,” *dreuz.info*, February 14, 2017, https://tinyurl.com/y6fkjodg

[68] Nicolas Vanderbiest, interviewed by Pauline Moullot, “Nicolas Vanderbiest: ‘WikiLeaks joue clairement un role dans la propagation des Macronleaks,’ ” *Libération*, May 6, 2017. See also Nicolas Vanderbiest, “Quelle est l’influence russe sur la campagne présidentielle française?” *reputatiolab.com*, April 20, 2017.

[69] Kevin Limonier and Louis Pétiniaud, “Mapping Cyberspace: The Example of Russian Informational Actions in France,” in *DRUMS: Distortions, Rumours, Untruths, Misinformation, and Smears*, ed. Norman Vasu, Benjamin Ang, and Shashi Jayakumar (Singapore: World Scientific, 2019), 55.

[70] *Ibid*., p. 60.

[71] Ben Nimmo *et al*., “Hashtag Campaign: #MacronLeaks: Alt-right attacks Macron in last ditch effort to sway French Election,” *DFRLab*

conversation using #MacronLeaks was dominated by the anti-Macron voices but a shift happened overnight, which coincided with a shift in language: at the same time the conversation became more French (on Saturday morning, seven of the ten top tweets were in French),[72] it also became more critical of the leak. The same day (Saturday), Nimmo, who was one of the first to analyze what was happening, observed that “the share of alt-right and anti-Macron messaging, which dominated the conversation initially, was progressively reduced by counter-messaging, either mocking the leaks and leakers or linking them to Russia.”[73] Therefore, the performance of the hashtag #MacronLeaks (almost half a million tweets in twenty-four hours) does not reflect the adherence of the users. As a matter of fact, as Nimmo guessed before the vote, this widespread campaign on Twitter failed to reshape the French political landscape.[74]

The leaked documents were mostly drawn from the hacked email accounts, but they also included two additional folders. One contained thirty-two Excel bookkeeping spreadsheets from Cédric O, the campaign treasurer. The other, named “Macron_201705” as if it contained fresh data on Macron (201705 being May 2017), contains instead old data on something else: documents dating from 2002 related to Gemplus, the world’s largest manufacturer of SIM cards, and to Ziad Takieddine, an outspoken Lebanese-French businessman. At that time Macron was a twenty-five-year-old student and had nothing to do with either Gemplus or Takkieddine. This unrelated folder, with an intentionally misleading title, was enough to trigger fanciful rumors, such as one claiming that, through Takkiedine, Macron was actually working with the Islamic State of Iraq and the Levant (ISIS)! One tweet, retweeted almost two thousand times, read: “#MacronLeaks Macron_201705 files show #Macron emails w/ Ziad Takieddine a Lebanese Arms Dealer. Could Macron be arming ISIS in #France?”[75]

Because nothing incriminating was found in the original files, which were therefore unlikely to harm Macron, the hackers had altered some of them in an attempt to discredit his campaign. The Macron leaks therefore fall into the category of “tainted leaks,” where (at least some of) the documents obtained are manipulated before being released.[76] The fake messages insinuated that Macron used cocaine (“don’t forget to buy c. for the boss”) and was on the mailing list of “Vestiaire Gay,” a gay underwear brand.

5. IN SUMMARY, A CLASSIC “HACK AND LEAK” INFORMATION OPERATION

A French cybersecurity researcher going by the name of “x0rz” summarized the information operation cycle as follows: “disinformation (media coverage) → Acquiring secret information via HUMINT or SIGINT (hacking) → Building a narrative around that information (optional: mix with fake/decoy information) → Releasing parts to social networks and press” (the last step feeding the first in a cycle)[77]. The Macron Leaks operation is a classic illustration of such a cycle.

The last step can be detailed in the following pattern: first, the content was dumped onto the political discussion board of 4chan (/pol/). Second, it was brought to mainstream social networks like Twitter. Third, it was spread through political communities, notably the US alt-right and French far-right, with catalyst accounts, or “gurus”, and finally the content was retweeted by both real people (“sect followers”)[78] and bots.

> *“…the hashtag’s persistence has not hurt the Macron administration, which has even sometimes turned it to its advantage.”*

It was obvious that bots were in use, as some accounts posted almost one hundred-fifty tweets per hour.[79] Nimmo identified fifty accounts that produced some

Medium.com, May 5, 2017 https://tinyurl.com/yy9jrmqy

[72] Ben Nimmo, “Resistance: French internet users mock alt-right US twitter storm,” *DFRLab Medium.com*, May 6, 2017, https://medium.com/dfrlab/macronleaks-campaign-hits-resistance-4fa490e4ae55.

[73] *Ibid*.

[74] *Ibid*.

[75] *Ibid*.

[76] Hulcoop *et al*., “Tainted Leaks.”

[77] x0rz, “Hacking (Back) and Influence Operations”, Medium.org, 18 April 2019.

[78] 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, 42.

[79] Nimmo *et al*., “Hashtag Campaign.”

3,801 tweets in the first three hours, which certainly seems to be bot amplification.[80] Overall, data scientist Emilio Ferrara identified nearly eighteen thousand bot accounts involved. According to his analysis:

> Many bot accounts that supported alt-right narrative in the context of #MacronLeaks were originally created shortly prior to the 2016 US presidential election and used to support the same views in the context of American politics. The accounts went dark after November 8, 2016, only to re-emerge at the beginning of May 2017 to push #MacronLeaks, attack Macron, and support the far-right candidate Marine Le Pen. This corroborates a recent hypothesis about the existence of black markets for reusable political botnets.[81]

A few months later, on July 31, 2017, WikiLeaks published “a searchable archive” of 21,075 “verified” leaked emails on a dedicated webpage (“Macron Campaign Emails”)[82]—something that the American far-right political activist Charles C. Johnson did as early as the day after the dump: “Chuck Johnson has developed a search engine for #MacronLeaks. Contact editor@gotnews.com for access” tweeted Posobiec on May 6.[83] Three months later, when WikiLeaks launched its own search engine, Sputnik and RT preceded the usual American alt-right amplifiers in retweeting the “urgent” and “breaking news.” Posobiec reacted a few hours later, using the hashtag he originally introduced in May: “#MacronLeaks is back.”

The role of WikiLeaks in the entire sequence is difficult to characterize. On the one hand, a study has shown that “three of the most retweeted tweets derived from WikiLeaks, and the WikiLeaks account was highly influential overall in covering the affair. … WikiLeaks ranked as the number one most influential user.”[84] Since the DNC leaks, WikiLeaks has been accused of being aligned with Russian intelligence. In his first speech as Central Intelligence Agency (CIA) director, on April 13, 2017, Mike Pompeo said, “It’s time to call out WikiLeaks for what it really is: a nonstate hostile intelligence service often abetted by state actors like Russia.” During the presidential campaign, he said “Russian military intelligence, the G.R.U., had used WikiLeaks to release data of US victims that the G.R.U. had obtained through cyberoperations against the Democratic National Committee.”[85] On the other hand, WikiLeaks’ role in the Macron leaks was more ambivalent and less catalytic than it had been in the United States. It helped both to spread the leak and to generate public skepticism by tweeting comments like, “This massive leak is too late to shift the election. The intent behind the timing is curious.”[86] WikiLeaks’ detachment helped to block the information-laundering process.

6. EPILOGUE: ONE AND TWO YEARS LATER

One year later, on May 5, 2018, Belgian researcher Nicolas Vanderbiest uncovered that, of the 1,654 actors most involved at the time in the circulation of the Macron leaks on Twitter, 1,263 (76 percent) were not French, and 428 (26 percent) disappeared after the incident. Some of these accounts were deactivated as early as one week after the election: one hundred seventy accounts were suspended by Twitter, and 249 were self-deleted or renamed by the user.[87]

However, even today, two years after its introduction, the hashtag #MacronLeaks is still in use as a rallying flag by the political opposition. It is regularly used either to comment on some specific information found in the emails, most notably regarding the campaign’s financing, or as a general tag to attack Macron, his government, and his political party, La République en marche (LREM).

Interestingly, the hashtag’s persistence has not hurt the Macron administration, which has even sometimes turned it to its advantage. After all, by revealing more than

[80] Ben Nimmo at the 360/OS Open Source Summit in Warsaw, July 5, 2017.

[81] Emilio Ferrara, “Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election, *First Monday*, 22:8, 2017, https://firstmonday.org/ojs/index.php/fm/article/view/8005/0.

[82] WikiLeaks, “Macron Campaign Emails,” July 31, 2017, https://wikileaks.org/macron-emails/.

[83] Jack Posobiec Twitter account, 6 May 2017, 4:39 pm.

[84] Ahmed and Downing, “Campaign leaks and the far-right.”

[85] Matthew Rosenberg, “Mike Pompeo, Once a WikiLeaks Fan, Attacks It as Hostile Agent,” *The New York Times*, April 13, 2017.

[86] WikiLeaks, “#MacronLeaks assessment update: This massive leak is too late to shift the election. The intent behind the timing is curious,” Twitter Account, May 5, 2017, 2:12 p.m. https://twitter.com/wikileaks/status/860603123236315137.

[87] Nicolas Vanderbiest, “Il y a un an, avait lieu les #MacronLeaks. Sur les 1654 importants protagonistes (au moins 1 RT, ou 3 tweets individuels): 428 ont aujourd’hui disparu, soit 26%. Preuve que les #FakeNews sont avant tout une affaire de désinformation. Analyse plus complète en cours.” Twitter Account, May 5, 2018, 10:53 a.m. https://twitter.com/Nico_VanderB/status/992824582729068544 and “Allez quand même le petit chiffre sur les #MacronLeaks 170 suspendus par Twitter (10 % des comptes), 249 comptes auto-supprimés ou pseudo changé par leur utilisateur, 1263 n’étaient pas français (76 %)” Twitter Account, May 5, 2018, 11:28 a.m. https://twitter.com/Nico_VanderB/status/992833422358994945

twenty-one thousand emails of Macron's campaign team, the leak subjected his candidacy to a level of transparency that none of his rivals had to endure—yet nothing incriminating was found on Macron, while some of his rivals, including Le Pen, were and still are facing legal problems. As early as May 6, 2017, half a day after the leak was released, an En Marche! activist tweeted, "#MacronLeaks The National Front and the Russians have achieved a magnificent exploit: confirming Macron's honesty. Thanks for your cooperation."[88] Exactly one year after, on May 6, 2018, Marlène Schiappa, the secretary of gender equality, tweeted, "Our campaign accounts have been scrutinized and certified. With the #MacronLeaks even our personal emails have been made public: we are the only ones to have reached this level of transparency! Everything is clear and has been validated by the authorities."[89]

[88] Adia, "#Macronleaks Le FN et les Russes ont réussi un magnifique exploit: confirmer l'honnêteté de Macron. Merci pour votre coopération," Twitter Account, May 6, 2017, 4:43 a.m. https://twitter.com/adia66/status/860822215406833664.

[89] Marlene Schiappa., "Nos comptes de campagne ont été examinés à la loupe et certifiés. Avec les #MacronLeaks même nos mails personnels ont été rendus publics: nous sommes les seuls à avoir atteint ce niveau de transparence! Tout est clair et validé par les instances, #LeGrandRDV" Twitter Account, May 6, 2018, 2:33 a.m. https://twitter.com/MarleneSchiappa/status/993061298438070273

II- WHO DID IT?

There were three distinct dimensions to the operation: the disinformation campaign (composed of rumors, fake news, and forged documents), the hack, and, finally, the leak. Even though they seem to be coordinated, these are "different acts and not a composite act."[90] They should therefore not be presumed to have one single actor behind them.

1. THE DISINFORMATION CAMPAIGN

Attributing the disinformation campaign is the easiest part as it was conducted overtly: as seen in the previous pages, the anti-Macron propaganda came mostly from two sources, RT and Sputnik on the one hand, and the American alt-right on the other.

It is then no surprise that, as early as February 2017, the En Marche! team attributed the orchestrated campaign against their candidate to the Kremlin. On February 13 on national television, Richard Ferrand, secretary-general of En Marche!, accused Russia, stating, "Two major media outlets, Russia Today and Sputnik, which belong to the Russian state, operate by the dissemination of fake news. Then, this news is spread, quoted, and assumes a role in the life of our democracy." He also denounced "hundreds, even thousands, of attacks on our digital system, on our database, on our sites. And coincidentally these come from within Russian borders."[91] A few minutes later on another public media outlet, En Marche! spokesman Benjamin Griveaux blamed RT and Sputnik again, saying, "The[se] two sites, for the last several weeks, have slandered candidates, including Emmanuel Macron, and bolstered Marine Le Pen. Russia had a role in the US presidential campaign by supporting Donald Trump, Brexit, and the campaign in Britain. It is now interfering in the French presidential campaign and it is not normal."[92]

On February 14, in an editorial in the *Le Monde* newspaper titled "Do not let Russia destabilize the presidential elections in France," Ferrand was once again clear as to whom he held responsible for the attacks:

> A new and worrying phenomenon is underway at the heart of the French presidential election: the interference of a foreign state determined to destabilize one of the candidates likely to win this election, Emmanuel Macron. … The website of the movement En Marche! and its infrastructure is subject to several thousand monthly attacks that come in various forms. The goal is to infiltrate our databases and our mailboxes in order to hack them. … Almost half of these attacks come from Ukraine.[93] What is certain about the nature of these attacks is that they are organized and coordinated by a structured group, not by solitary hackers. … For several weeks now, Russia Today and SputnikNews have been busy spreading the most libelous rumors about Emmanuel Macron. One day, he is financed by "the rich gay lobby," another, he is an "American agent at the service of the banking lobby." These two sites are the preferred medium for all attacks suffered by Emmanuel Macron, including threats by Julian Assange. … Cyberattacks, threats made by a hacker protected by a foreign power, attempts to undermine and defame made by news sites funded by this same foreign power, the coordinated relay of this false information on social networks: we are in the presence of an orchestrated attempt to destabilize a presidential candidate by a foreign power.[94]

The following day, February 15, Foreign Minister Jean-Marc Ayrault was more measured, telling parliament that France would not tolerate any interference in its electoral process, "no more from Russia than from any other state."[95]

[90] François Delerue, *Cyber Operations and International Law* (Cambridge University Press, 2019, forthcoming), section 5.4 on "Cyber operations and the principle of non-intervention and non-interference."

[91] "L'équipe de Macron persuadée d'une ingérence russe dans sa campagne," *Le Parisien*, February 13, 2017.

[92] *Ibid*.

[93] As noticed by Kevin Limonier and Colin Gérard, this does not prove anything, as "Ukraine is a hotbed of malicious proxies allowing hackers, wherever they are in the world, to hide their tracks" ("Guerre hybride russe dans le cyberspace," *Hérodote*, 166-167, 2017/3, 162).

[94] Richard Ferrand, "Ne laissons pas la Russie déstabiliser la présidentielle en France!" *Le Monde*, February 14, 2017, https://www.lemonde.fr/election-presidentielle-2017/article/2017/02/14/ne-laissons-pas-la-russie-destabiliser-la-presidentielle-en-france_5079213_4854003.html.

[95] Martin Untersinger, "Cyberattaques: la France menace de 'mesures de rétorsion' tout Etat qui interférerait dans l'élection," *Le Monde*, February 15, 2017, https://www.lemonde.fr/pixels/article/2017/02/15/cyberattaques-la-france-menace-de-mesures-de-retorsion-tout-etat-qui-interfererait-dans-l-election_5080323_4408996.html

As a matter of fact, the disinformation campaign was also coming from the US alt-right, as clearly demonstrated in the first part of this report. That was particularly clear on digital platforms. A research unit[96] analyzed a corpus of four hundred-thousand tweets unambiguously attacking Macron, posted between February 1 and May 6. Time zone analysis indicates that most of them came from abroad, in particular North America.[97] As for the fake LeSoir.info website, it has been registered by a “Donald Thomas” providing a fake address (Apple street instead of Orange street) in Wilmington, Delaware. The same address has been used to register three other cloned websites: indepnedent.co, alryiadh.com, and bloomberq.com. People citing those domains seem to be systematically pro-Trump, pro-Putin, pro-Assad, pro-Brexit, and anti-EU.

As for the #MacronGate rumor, the Bulgarian investigative website Bivol, which analyzed the metadata of the two fake PDFs, showed they were last modified at 10:27 a.m. on May 3 (the day they were dumped). They further showed that these documents were scanned using two professional Canon machines, costing $29,999 and over $100,000 respectively. Bivol concluded that “the masterminds of the discrediting claim have access to high-end equipment that is used by large companies or institutions. … In addition, metadata may be manipulated, which is impossible to prove, but such manipulation would also be a sign of high professionalism, not an amateur forgery concocted by Macron’s opponents and Le Pen’s fans.”[98]

The internet user responsible for the #MacronGate rumor, which occurred two days before the leak, may in fact be an American neo-Nazi hacker. Shortly after posting the fake documents on 4chan that supposedly showed that Macron had a hidden offshore bank account, the user with a Latvian IP address wrote the following message: “if Macron wins we’re gonna have to organize and make things happen. The French scene will be at nouveaumartel.com later.” Nouveau Martel (New Martel) refers to Charles Martel, an eighth-century Frankish ruler (grandfather of Charlemagne) famous for having defeated the Arabs near Poitiers in 732, and therefore hailed by some as having saved Christian Europe from a Muslim invasion. For this reason, Martel is commonly invoked by the French far-right movements. At the time this leaker posted the link, the nouveaumartel.com website was empty–and remains so. However, an investigation showed that it shared the technical infrastructure of The Daily Stormer, one of the main American neo-Nazi websites. The tech administrator of nouveaumartel.com was “weev,” a nickname used by Andrew Auernheimer,[99] a white-supremacist, anti-Semitic American hacker who gained notoriety three years earlier when a US appeals court vacated his conviction for computer fraud. On May 5 on 4chan, only minutes after the publication of the high-definition version of one of the #MacronGate fake documents, two comments were posted to congratulate “weev.” The day before, in an article published on his website, he wrote that “The prophet of the white sharia Nathan Damigo is about to release the frogs from pederasty”, which can be interpreted as an announcement “that Damigo was about to publish anti-Macron material”.[100] Indeed, Damigo will be the first person to spread the #MacronGate rumor on Twitter. As *Le Monde* concludes, “a cluster of concordant indices shows that members of Anglophone neo-Nazi circles are probably at the origin of the publication of false documents accusing Emmanuel Macron of holding an offshore account,” i.e. the #MacronGate episode.[101]

2. THE HACK

The disinformation campaign was easy to attribute. However, it is much more difficult to determine responsibility for the hack itself, which resulted in the theft of gigabytes of data. In any cyberattack, attribution is a complex and sensitive issue.

Take, for instance, the fake domains used for (at least some of) the phishing attacks (onedrive-en-marche.fr, mail-en-marche.fr, portal-office.fr, and accounts-office.fr). We know that they were registered between March

[96] *Institut des systèmes complexes de Paris IDF*, from the French National Center for Scientific Research (*Centre national de la recherche scientifique*), a governmental research organization.

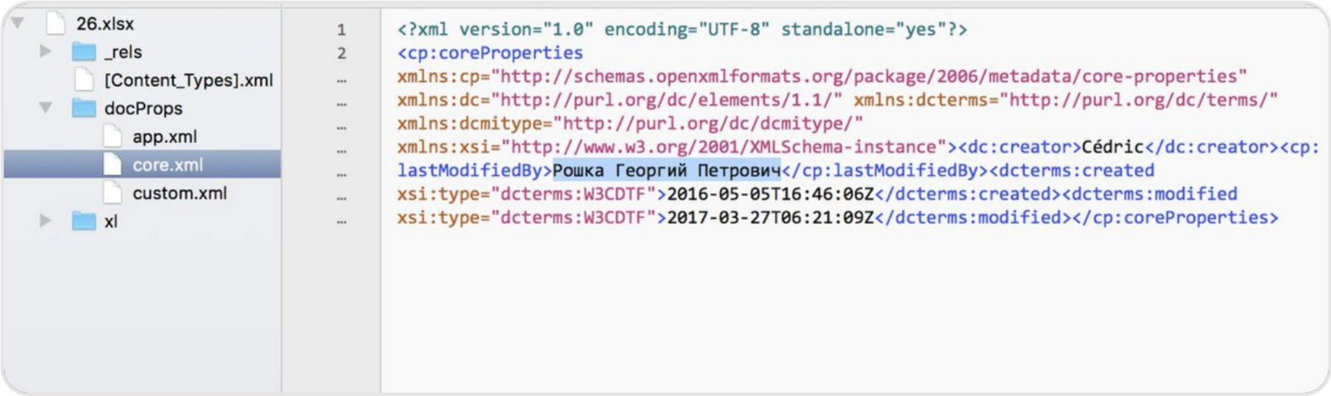
[97] David Chavalarias, Noé Gaumont, Maziyar Panahi, “Avis de tempête sur notre démocratie,” *politoscope.org*, May 5, 2017. See also David Chavalarias, “Le ‘putsch final’ sur notre démocratie va-t-il réussir?” politoscope.org, May 6, 2017.

[98] Bivol.bg, “‘Canon’ for Macron: The fake news on Emmanuel Macron offshore account looks too professional,” *bivol.bg*, May 5, 2017. https://bivol.bg/en/canon-for-macron.html

[99] “Tracing the Source of MacronGate, the Macron Offshore Papers,” *Qurium*, undated, and David Gauthier-Villard, “US Hacker Linked to Fake Macron Documents, Says Cybersecurity Firm,” *The Wall Street Journal*, May 16, 2017, https://www.wsj.com/articles/u-s-hacker-linked-to-fake-macron-documents-says-cybersecurity-firm-1494929136.

[100] Andrew Rettman, “US neo-Nazis linked to Macron hack”, *EU Observer*, 12 May, 2017. https://euobserver.com/foreign/137882

[101] Damien Leloup and Martin Untersinger, “ ‘MacronLeaks,’ compte offshore : l’ombre des néonazis américains,” *Le Monde*, May 11, 2017, https://www.lemonde.fr/pixels/article/2017/05/11/macronleaks-compte-offshore-d-emmanuel-macron-l-ombre-des-neonazis-americains_5126389_4408996.html.



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<cp:coreProperties
xmlns:cp="http://schemas.openxmlformats.org/package/2006/metadata/core-properties"
xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:dcterms="http://purl.org/dc/terms/"
xmlns:dcmitype="http://purl.org/dc/dcmitype/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><dc:creator>Cédric</dc:creator><cp:
lastModifiedBy>Рошка Георгий Петрович</cp:lastModifiedBy><dcterms:created
xsi:type="dcterms:W3CDTF">2016-05-05T16:46:06Z</dcterms:created><dcterms:modified
xsi:type="dcterms:W3CDTF">2017-03-27T06:21:09Z</dcterms:modified></cp:coreProperties>
```

The Excel bookkeeping spreadsheets that were leaked contained metadata in Cyrillic and indicate that the last person to have edited the files is “Рошка Георгий Петрович” (Roshka Georgiy Petrovich), *Photo credit: WikiLeaks*

15 and April 17, three of them with a Ukrainian and one with a French phone number[102], but the numbers do not tell us who registered them, and even if they did, this person may be disconnected from those who actually carried out the attacks. Some operations are so compartmentalized that people in one part of it may not know for whom or what they work ultimately. And the “evidence” we find afterward can be fabricated. Attribution is a puzzle with a lot of unknowns. It is, ultimately, a political decision, based on technical elements, but most of the time without certainty. Some states, like the United States, and consequently their Five Eyes allies, are not hesitant to attribute. Others, like France, are more prudent. At the time of writing, two years after the incident, France still has not publicly attributed the attacks to any particular perpetrator, as is its custom (the 2015 cyberattack against France’s TV5Monde has not been attributed either, see below). Other nonstate actors, however, have not been so coy.

“Attribution is a puzzle with a lot of unknowns. It is, ultimately, a political decision”

In early February, the famous information security researcher “The Grugq,” who predicted the leaks against Macron, wrote, “For months I’ve been hearing from credible sources that Russian cyber crews (Sofacy, APT28, etc.) have been collecting aggressively in France. … They have been conducting stepped up cyber espionage against the French since last year.”[103] In his expert opinion, it was a Russian operation, and its preparation, the collecting of the data, started in 2016.

In April, Trend Micro, the Japanese cybersecurity firm that identified the March 15 phishing attack, attributed it to APT28 (also known as Fancy Bear or Pawn Storm), a cyberespionage group linked to the Russian military intelligence agency GRU.[104] It would not be the first time that APT28 attacked a French institution. In 2015, the American cybersecurity firm FireEye attributed responsibility for the cyberattack against TV5Monde to them. In that false-flag operation, the attackers took the channel off the air and tried to frame the so-called Islamic State for it by displaying “Cyber Caliphate” banners on the channel’s websites.[105]

In 2017, Trend Micro identified “the same actors as in the DNC breach” and “similar techniques” to those used to target Angela Merkel’s political party, the Christian Democratic Union (CDU), in 2016.[106] “There are several things which suggest that the group behind the Macron hacking was also responsible for the DNC breach, for example. We found similarities in the IP addresses and malware used in the attacks. … We

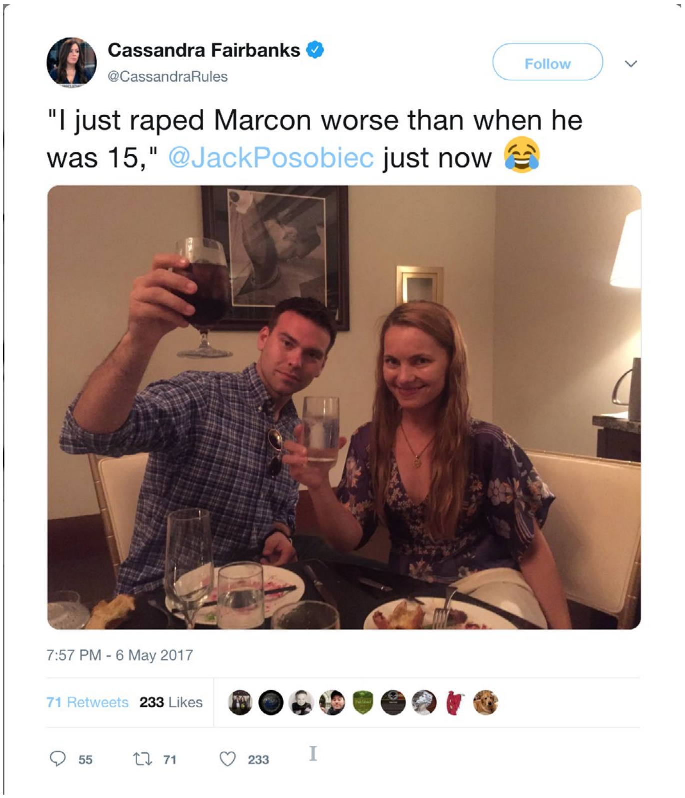
[102] Martin Untersinger, “La campagne d’Emmanuel Macron dans le viseur de pirates russes,” *Le Monde*, April 25, 2017, https://www.lemonde.fr/pixels/article/2017/04/25/la-campagne-d-emmanuel-macron-dans-le-viseur-de-pirates-russes_5117304_4408996.html.

[103] thaddeus t. grugq, “Opening Cyber Salvo in the French Elections,” *Medium.com*, February 6, 2017.

[104] Hacquebord, *Two Years of Pawn Storm*, 13.

[105] Sam Schechner, “France Says Evidence Suggests Russians Posing as Islamists Hacked Broadcaster,” *The Wall Street Journal*, June 10, 2015, https://www.wsj.com/articles/france-says-evidence-suggests-russians-posing-as-islamists-hacked-broadcaster-1433955381.

[106] Eric Auchard, “Macron campaign was target of cyberattacks by spy-linked group,” Reuters, April 24, 2017, https://www.reuters.com/article/us-france-election-macron-cyber/macron-campaign-was-target-of-cyber-attacks-by-spy-linked-group-idUSKBN17Q200.



Cassandra Fairbanks
@CassandraRules

"I just raped Marcon worse than when he was 15," @JackPosobiec just now 😂

7:57 PM - 6 May 2017

71 Retweets 233 Likes

55 71 233

Cassandra Fairbanks, a famous pro-Trump political activist, Sputnik contributor, and “troll,” posted on Twitter a picture of Jack Posobiec celebrating (apparently with her and his wife). *Photo Credit: Twitter*

cannot say for sure whether this was directed by the Russian government, but the group behind the attacks certainly appears to pursue Russian interests,” said Rik Ferguson, vice president of Trend Micro’s security research program.[107] Trend Micro warned that Fancy Bear “is known to let time pass before leaking stolen documents”[108] and that is indeed what happened.

The cybersecurity experts of the ThreatConnect research team established that the four spoofed domains were registered using the email address johnpinch@mail.com—an email domain that Fancy Bear has previously used in similar operations. “While not definitive of a Fancy Bear association, it is a notable consistency with their previous tactics.”[109] Another clue is that they were all registered on dedicated servers, a practice that is costlier but gives more control. At least one of these domains was hosted at the IP 194.187.249.135, an address that was already identified in the 2016 US Department of Homeland Security Grizzly Steppe report on Russian malicious cyber activity. ThreatConnect found that the address was previously a Tor exit node and identified other consistencies “with Fancy Bear registration and hosting tactics”.

However, a method indeed but not solely employed by Fancy Bear does not give any certainty regarding attribution. ThreatConnect concludes that they “cannot currently definitively confirm Trend Micro’s assessment that Fancy Bear aka Pawn Storm is behind this activity.” For the same reasons, France did not officially attribute the hacking. “The modus operandi is very similar [to APT28], but we cannot exclude that a very competent group can try to imitate them,” said Guillaume Poupard, the head of the French National Cybersecurity Agency (ANSSI).[110]

The Macron campaign staff reacted to the publication of the Trend Micro report between the two rounds of the presidential election, on April 25, 2017. Spokesman Griveaux said that “2,000 to 3,000 attempts have been made to hack the campaign, including denial-of-service attacks that briefly shut down Macron’s website and more sophisticated efforts to burrow into email accounts of individual campaign workers. He was not sure whether Macron had been targeted personally and said the main target of the phishing appears to have been the campaign’s mid-level management.”[111] Earlier in February, Mahjoubi observed, “Half of the attacks that target us come from IP addresses based in Ukraine, a relay country for many cyberattacks.”[112] Reacting to the Trend Micro report, he confirmed that “these attacks are constant and of all variety, including phishing attacks, since December, January. ... [We have counted] several thousand connections that can be tied to these attacks each month. We were unable to attribute them and that is what this report does, it confirms the intuition we have had since February. But let us not be naïve either: in terms of cyberattacks, a group of hackers can also act on behalf of a larger group or in others’ interests. The only way to know

[107] Rick Noack, “Cyberattack on French presidential front-runner bears Russian ‘fingerprints,’ research group says,” *The Washington Post*, April 25, 2017.

[108] Auchard, “Macron campaign was target.”

[109] ThreatConnect research team, “Parlez-vous Fancy?”, Threatconnect.com, 26 April 2017.

[110] Guiton, “En marche, cible des hackers de Fancy Bear?”

[111] Noack, “Cyberattack on French presidential front-runner.”

[112] Mahjoubi, quoted in “Présidentielles: face aux cyberattaques, les équipes de campagne renforcent leur sécurité,” *20minutes.fr*, February 14, 2017.

would be to investigate, and a presidential campaign is not the time for that.”[113]

Another source of evidence is Facebook. During a briefing to a US congressman, Facebook officials reportedly said that they had identified about two dozen Facebook accounts created to conduct surveillance on Macron’s entourage during the campaign. Furthermore, they appeared to know that these accounts were run by “Russian agents posing as friends of friends of Macron associates and trying to glean personal information from them.” They also understood that the agents’ goal was “to get the targets to download malicious software or give away their login information.”[114]

3. THE LEAK

In the days and weeks following the release of the hacked data, most experts pointed to the Kremlin, with good reason. First, the email address initially used to upload the files on Archive.org, frankmacher1@gmx.de, is registered with the same German webmail provider that was implicated in the 2016 cyberattack against the CDU,[115] which incidentally was also attributed to APT28.[116] Of course, this alone proves nothing, as GMX Mail has more than eleven million active users.

Second, according to Ryan Kalember of information security firm Proofpoint, “Some of the metadata from this breach clearly indicates that certain documents, such as those with Macron’s ‘Bahamian bank accounts’, were edited on computers with Russian language operating systems.”[117] The Excel bookkeeping spreadsheets that were leaked contained metadata in Cyrillic and indicate that the last person to have edited the files is “Рошка Георгий Петрович” (Roshka Georgiy Petrovich), reportedly an employee of the St. Petersburg-based information technology company Evrika ZAO. Among the company’s clients are several government agencies, including the Federal Security Service of the Russian Federation (FSB).[118] Moreover, the Russian independent newspaper *The Insider* found Roshka in the participants’ list for a 2016 conference where he was registered as “Military unit No. 26165, specialist,” “also known as GRU 85 Main Special Service Center dedicated to cryptoanalysis.” Their conclusion is that “the people involved in hacking Macron’s email were directly related to the Russian government: they were officers of the Main Intelligence Directorate of the Russian Armed Forces (GRU).”[119]

“France did not officially attribute the hacking”

It is difficult, though, to infer anything certain from this connection. It could have been a false-flag operation intended to misdirect and falsely incriminate Moscow. Rob Graham, a cybersecurity consultant, notes, “Obviously if I’d done it, I’d go to the .xml files and set this up for people to find it. … We all believe it’s probably Russia, but this really isn’t evidence that it is Russia.”[120]

Third, Kremlin propagandist Konstantin Rykov, sometimes nicknamed the “chief troll,” who boasted of his role in Trump’s election,[121] also acknowledged failing with Macron. “We succeeded, Trump is president. Unfortunately, Marine did not become president. One thing worked, but not the other,”[122] he mused. Such a confession is troubling but cannot be taken as sufficient evidence because “we” can refer to various groups, not all of them connected to the Kremlin.

Similarly, on the other side of the Atlantic on Saturday, May 6, the day after the dump and before the final round of the

[113] Mahjoubi, quoted in “En Marche! cible d’une tentative de hameçonnage par les Russes,” *L’OBS*, April 25, 2017.

[114] Joseph Menn, “Exclusive: Russia used Facebook to try to spy on Macron campaign–sources,” Reuters, July 27, 2017, https://www.reuters.com/article/us-cyber-france-facebook-spies-exclusive/exclusive-russia-used-facebook-to-try-to-spy-on-macron-campaign-sources-idUSKBN1AC0EI.

[115] Sean Gahhagher, “Evidence suggests Russia behind hack of French president-elect,” *Ars Technica*, May 8, 2017, https://arstechnica.com/information-technology/2017/05/evidence-suggests-russia-behind-hack-of-french-presidential-candidate/.

[116] Feike Hacquebord, “Pawn Storm Targets German Christian Democratic Union,” *TrendLabs Security Intelligence Blog*, May 11, 2016.

[117] Alex Hern, “Macron hackers linked to Russian-affiliated group behind US attack”, *The Guardian*, 8 May 2017.

[118] Gahhagher, “Evidence suggests.”

[119] Roman Dobrokhotov, “Roshka the Bear. How French president’s mailbox was hacked by Russian intelligence,” *The Insider*, October 28, 2017, https://www.4freerussia.org/roshka-and-russian-hackers-the-gru-broke-into-french-presidents-mail-box/

[120] Andy Greenberg, “Don’t Pin the Macron Email Hack on Russia Just Yet,” *Wired*, May 8, 2017, https://www.wired.com/2017/05/dont-pin-macron-email-hack-russia-just-yet/

[121] On his Facebook page: “I’ll tell you about (now it’s possible) how Donald Trump and I decided to free America and make it great again. This took us as much as 4 years and 2 more days,” November 12, 2016. See Scott Stedman, “Kremlin Propagandist Boasted of His Hacking Efforts, Strongly Implied Colluding With Trump Team in Facebook Posts,” *Medium.com*, November 21, 2017.

[122] Konstantin Rykov in a mediametrics.ru interview, in the documentary *La guerre de l’info*.

presidential election, Cassandra Fairbanks, a famous pro-Trump political activist, Sputnik contributor, and "troll,"[123] posted on Twitter a picture of Jack Posobiec celebrating (apparently with her and his wife) and quoted him as saying, "I just raped Marcon [*sic*] worse than when he was 15."[124] However, he could have been simply boasting of his role in contributing to the Macron leaks by retweeting and spreading them. Almost two years later, in a March 29, 2019, tweet, Posobiec boasts and laments at the same time: "#Macronleaks is the biggest story I've ever broken … Yet the media refuses to refer to me as 'the Macronleaks guy.'"[125] He regrets that only two outlets have ever done so, *The New Yorker* and *The Atlantic*, "But since 2017, the media seems to have dropped the label. Whenever they write about me, they misleadingly OMIT the biggest story I have ever broken." Comparing himself to a "comet" threatening the "legacy media dinosaurs," he thinks that they are simply jealous that he, who is not "an approved journalist," was able to leak "a massive story [and] obtain protected information." In other words, that he can do "what they do; better, faster and cheaper." Why? Because, he adds: "Spoiler alert: I'm a former intelligence officer trained in HUMINT. I know how to do this."

His role in the "Macron Leaks" operation is a feat of arms that Posobiec likes to highlight. It is even part of his identity: during some time, he presented himself in his Twitter profile as "Catholic. National security conservative. Veteran Intel Officer. *Macronleaks*." As a matter of fact, this episode did contribute to increase his exposure. At the exact same time he was campaigning against Macron, he was given White House press accreditation, a temporary access in early April 2017, and he attended his first daily press briefing only a few days after he contributed to the "Macron Leaks" operation.[126] Two years after, he more than quadrupled the number of followers he had at the time.

While being certainly an interesting character, Posobiec's importance in the Macron Leaks operation should not be overestimated. He was indeed the first to use the hashtag #MacronLeaks but not the first to break the story. In the case of the #MacronGate on May 3, Nathan Damigo and his neo-Nazi network were the first to break the story, then Craddick, and then only Posobiec who, with eleven times more followers, amplified it. As Stéphanie Lamy noticed, in the case of the #MacronLeaks on May 5, the division of labor was similar: Craddick was the first to break the story, and Posobiec the first to amplify it. Therefore, Posobiec is interesting to the extent that he was the first amplifier.

"France is known to be fertile ground for Russian influence"

Craddick is even more interesting. Indeed, there are reasons to believe that Craddick was not only the first to break the story, but actually the one who posted the files on 4chan – or if not him personally, someone working with him. After he announced, at 7:37 pm, "Prepare for a major leak on Emmanuel Macron and his close associates", someone asked him: "Are you going to post on T_D?" (the subreddit The_Donald). He answered at 8:32 pm: "T_D, /pol/, and of course all of our official and staff social media. You won't have trouble finding it."[127] In other words, Craddick not only did not deny he was "going to post" it, but he even specified where. T_D was down at the time: "@thedonaldreddit is a no go. Servers are down ATM. Twitter links and /pol/ best place" observed another user. As a matter of fact, at 8:35 pm, three minutes after Craddick said he was going to post the links on /pol/, the links were indeed posted on /pol/. And, 15 minutes later, he was the first to tweet them. The IP address from where the files were posted on Twitter was not Latvian this time, but American and, in his message, the poster says the documents were "passed on" to him that day[128]. Therefore, if Craddick is (only) the poster, which is likely (Lamy is "99% sure")[129], the question is: where did he get the files from?

Lamy also concludes, amplifying Posobiec's role was probably not the smartest thing to do: focusing on Craddick would have been more relevant, and could

[123] Michelle Kaminsky, " 'Grassroots' Journalist Loses Defamation Suit Over Tweet Of Alleged White Power Hand Gesture," *Forbes*, June 8, 2018, https://www.forbes.com/sites/michellefabio/2018/06/08/grassroots-journalist-loses-defamation-suit-over-tweet-of-alleged-white-power-hand-gesture/#1b64747d7754

[124] Cassandra Fairbanks, "I just raped Marcon worse than when he was 15, @JackPosobiec just now," Twitter Account, May 6, 2017, 7:57 p.m. https://twitter.com/CassandraRules/status/861052299300528128.

[125] Jack Posobiec, "#Macronleaks is the biggest story I've ever broken 'In the final hours of the election Posobiec located a 9GB archive of Macron's emails, photographs, and internal documents' Yet the media refuses to refer to me as 'the Macronleaks guy' I can explain," Twitter Account, March 29, 2019, https://twitter.com/JackPosobiec/status/1111720381373657088

[126] Dustin Volz, "Commentator who amplified Macron hacks given White House press access", Reuters, 11 May 2017.

[127] Pauline Moullot, "Le premier internaute à avoir relayé les MacronLeaks est en fait William Craddick," *Libération*, May 8, 2017.

[128] Doman, "MacronLeaks".

[129] Stéphanie Lamy, "D'ailleurs, dans le deuxième cas c'est à 99% sur que c'est Craddick & team qui est corbeaux 4chan mais aussi celui qui a uploadé sur ARCHIVE". Twitter Account, May 11, 2017, https://twitter.com/WCM_JustSocial/status/862769616413757440

even have had the secondary effect of "create some friction between them"[130].

4. CONCLUSION: A COMBINATION OF RUSSIAN INTELLIGENCE AND AMERICAN ALT-RIGHT

France has never officially attributed responsibility for the cyberattack. On June 1, 2017, Guillaume Poupard, the ANSSI director, declared that "the attack was so generic and simple that it could have been practically anyone. … To say Macron Leaks was APT28, I'm absolutely incapable today of doing that. … I have absolutely no element to say whether it's true or false." What can be safely assumed is whoever the perpetrators were they were at least linked to Russian interests. They also received help from both the American alt-right and the French fachosphère, both of whom are pro-Russian. As Boris Toucas explained, "A plausible pattern is that, just like during the US electoral campaign, a combination of state (most likely Russia) and nonstate interests colluded to generate a media buzz, then disseminated by opponents to Macron, especially far-right groups." [131]

Defense minister, Jean-Yves Le Drian, on December 10, 2016, two days before announcement of the creation of a cyber command composed of 2,600 "cyber fighters." *Source: REUTERS/Hamad I Mohammed*

None of the previous elements *alone* proves anything but, taken together, they do indeed suggest that Moscow was involved. "Any one of these data points in and of themselves doesn't point us to APT28 or Russia. … But I think when you look at all these data points together, that's what led us to make that moderate confidence assessment that it was APT28," said Tom Hoffmann, vice president of intelligence for the American cybersecurity firm Flashpoint.[132] This can seem unsatisfying, but it is the nature of attribution. As Matt Tait, a cybersecurity fellow at the University of Texas at Austin, said, "Attribution is often a matter of iteratively establishing a model that best explains the available evidence. Thus far, the available evidence does lean conspicuously towards Moscow."[133] Professor Thomas Rid confirms that the attribution of cyberattacks is not an exact science: "I do think this is more likely than not a Russian operation, but I'd put this at more like 60 percent at this stage. … None of the pieces of evidence that has come out so far is particularly strong in forensic terms. We only have circumstantial evidence. We can't exclude the possibility that someone is trying to frame someone else. … We don't know. I would be very cautious at this point to try to make any strong attribution claims."[134]

These experts are right to insist that attribution is never a certitude. They acknowledge, however, that the available evidence in this case points toward Russia. This is no surprise. France is known to be fertile ground for Russian influence. It is considered "the most prominent example of Russia's soft power in Western Europe, due not only to the long-lasting positive bilateral relations but also to the presence of an important Russian emigration since the 1920s that can act as a relay of influence."[135] There are numerous studies on Russian networks and relays of influence in France, from

[130] Stéphanie Lamy, "Focaliser sur Craddick (plus juste) aurait aussi permis de dégonfler l'égo de Posobiec. Créer de la friction entre eux deux #disruption". Twitter Account, 9 May, 2017, https://twitter.com/WCM_JustSocial/status/861842797674065921

[131] Boris Toucas, *The Macron Leaks: The Defeat of Informational Warfare*, Center for Strategic & International Studies (CSIS), May 30, 2017, https://www.csis.org/analysis/macron-leaks-defeat-informational-warfare.

[132] Patrick Howell O'Neill, "Researchers link Macron hack to APT28 with 'moderate confidence," *Cyberscoop*, May 11, 2017, https://www.cyberscoop.com/researchers-link-macron-hack-to-apt28-with-moderate-confidence/

[133] Matt Tait, "The Macron Leaks: Are They Real, and Is It Russia?" *Lawfare*, May 8, 2017, https://www.lawfareblog.com/macron-leaks-are-they-real-and-it-russia.

[134] Greenberg, "Don't Pin the Macron Email Hack."

[135] Carnegie Council for Ethics and International Affairs, introducing a series of publications on Russia's influence in France: Marlène Laruelle, *Russian Soft Power in France: Assessing Moscow's Cultural and Business Para-Diplomacy, Carnegie Council*, January 8, 2018; and Nicolas Lebourg, *The French Far Right in Russia's Orbit, Carnegie Council*, May 15, 2018.

An art group of which Katasonova is a member produced a Soviet-style triptych of Putin, Le Pen, and Trump *Photo Credit: Bellingcat.com*

political parties across the spectrum, to journalists, businessmen, and cultural figures.[136]

> *“These two hypotheses—the Russian intelligence services and the American alt-right movements—are not mutually exclusive.”*

In the 2017 presidential election, it was no secret that Macron’s opponent, Le Pen, was the Kremlin’s favored candidate. In 2014, her party, the National Front, received a loan of €9.4 million from the First Czech-Russian Bank in Moscow. One month before the election, Le Pen traveled to Moscow to meet with Putin. She claimed it was their first meeting but it was their third.[137] This suggests that the Kremlin made a major “investment” in the National Front.[138] In addition, Le Pen was very popular in Russia. There was a “Women for Marine” movement, headed by Maria Katasonova,[139] a propagandist who became famous for a fake video of her on the Ukrainian front (in reality Katasonova was in a studio with simulated sounds of shelling explosions).[140] An art group of which Katasonova is a member produced a Soviet-style triptych of Putin, Le Pen, and Trump that Katasonova used for her unsuccessful campaign for election to the Duma with the far-right Rodina Party in 2016. In April 2017, a few weeks before the French election, she traveled to Paris and offered her triptych to Le Pen, who hung it in her headquarters.[141]

[136] 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).

[137] According to Pierre Malinowski, former adviser to Jean-Marie Le Pen, interviewed in the documentary *La guerre de l’info*.

[138] Comment by Moreira, *ibid*.

[139] See Max de Haldevang, “A glamorous young Russian nationalist is leading her country’s love affair with Trump and Le Pen,” *Quartz*, March 24, 2017, https://qz.com/941383/maria-katasonova-the-glamorous-young-russian-nationalist-leading-her-countrys-love-affair-with-trump-and-le-pen/.

[140] Oli Smith, “Russia’s fake Ukraine war report exposed in Putin PR disaster,” *StopFake.org*, August 26, 2015.

[141] Marc de Boni, “Dans son QG, Marine Le Pen représentée en peinture avec Trump et Poutine,” *Le Figaro*, April 14, 2017, http://www.

In its official press release at 11:56 p.m. on Friday, May 5 (see below), the Macron campaign did not attribute the “massive and coordinated hacking operation” against them to any particular perpetrator. But that did not stop some in the Macron team from doing so. In an interview conducted on the same day, Aurélien Lechevallier, Macron’s foreign policy adviser, said, “We will have a doctrine of retaliation when it comes to Russian cyberattacks.”[142] “Cyberhacks and info-ops would make you take a very dim view of the person governing Russia, even if you had no prejudices before you started campaigning,” added Francois Heisbourg, one of Macron’s defense advisers during the campaign. Similarly, Bruno Tertrais, another adviser to Macron’s campaign, argued that “the Russian attacks have backfired. … They have hardened him [Macron] … and they have hardened his views on Russia.”[143]

Even with all the circumstantial and contextual elements pointing to Russia, however, there are reasons to look West as well: as demonstrated in the previous pages, an important part of the disinformation campaign was conducted by the American alt-right. The person, or persons, behind the #MacronGate may be an American neo-Nazi, possibly Andrew Auernheimer, and William Craddick seems to be the 4chan poster of the leaks. Moreover, those leaks were amplified mostly from the US. A study of the online conversation in the days preceding the vote shows that “the three top sources of traffic [mentioning #MacronLeaks] were Reddit (36 percent of mentions), 4chan (34 percent of mentions), and 8chan (4 percent of mentions), all sites that are associated directly with the American alt-right. On the day of the #MacronLeaks spike, the amount of traffic coming out of the United States nearly equaled that from France (35.8 percent US-based and 39.5 percent French-based), suggesting that there was a concerted effort from US far-right and alt-right groups to influence the French election.”[144]

One month before the election, Le Pen traveled to Moscow to meet with Putin. She claimed it was their first meeting but it was their third. *Photo credit: Wikimedia Commons https://commons.wikimedia.org/wiki/File:Marine_Le_Pen_and_Vladimir_Putin_(2017-03-24)_01.jpg*

These two hypotheses—the Russian intelligence services and the American alt-right movements—are not mutually exclusive. The hacking and leaking could have been committed by two different people/organizations independently. Due to their convergence of interests, there may have been a de facto alliance between them.[145] Such an alliance could be conscious or not: as in the disinformation campaign, several actors coming from both the United States and Russia could have worked for the same result without necessarily working together. However, an interesting lead to investigate, as it may be the link between those two sides, is where Craddick got the files from.

lefigaro.fr/elections/presidentielles/2017/04/14/35003-20170414ARTFIG00187-dans-son-qg-marine-le-pen-representee-en-peinture-avec-trump-et-poutine.php

[142] Ben Judah, “Emmanuel Macron’s Foreign Policy Doctrine(s),” *Politico*, May 8, 2017. Interview conducted on May 5: https://twitter.com/b_judah/status/860621504211496962.

[143] *Ibid*.

[144] Jacob Davey, Erin Marie Saltman, and Jonathan Birdwell, “The Mainstreaming of Far-Right Extremism Online and How to Counter It: A Case Study on UK, US, and French Elections,” in *Trumping The Mainstream: The Conquest of Democratic Politics by the Populist Radical Right*, eds. Lise Esther Herman and James Muldoon (Routledge, 2018), 40.

[145] Casey Michel, “America’s neo-Nazis don’t look to Germany for inspiration. They look to Russia,” *The Washington Post*, August 22, 2017, https://www.washingtonpost.com/news/democracy-post/wp/2017/08/22/americas-neo-nazis-dont-look-to-germany-for-inspiration-they-look-to-russia/?utm_term=.60b896b39f12.

III- WHY DID IT FAIL AND WHAT LESSONS CAN BE LEARNED?

In short, the leak did not significantly influence French voters, despite the efforts of the aforementioned actors. As also noted by Toucas, it

> didn’t have nearly as much influence on the election campaign as the traditional journalism of one well-known French media outlet, *Le Canard Enchaîné*, which published revelations that marred François Fillon’s campaign. A respected satirical newspaper founded in 1915, *Le Canard Enchaîné* publishes incriminating stories on any political party and proudly refuses advertisements to ensure its independence. The effect of its reporting, which depended on seasoned journalists carefully evaluating and analyzing inside information, was far greater than the impact of a massive, indiscriminate dump of unverified files by the hackers.[146]

Why did the intrusion fail? How can this failure be explained? How did France withstand this election meddling? And, looking to the future, what lessons can be learned from this experience? As the following section will show, this success was due to a combination of structural factors, luck, and 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, France presented a less vulnerable political and media environment for a number of reasons. First, the length of the French presidential campaign is regulated: contrary to the United States, where presidential campaigns tend to become two-year marathons, in France the unofficial campaign starts one year before the first day of the month of the election (in this case, April 1, 2016), while the official campaign starts once the official list of candidates is established by the Constitutional Council (*Conseil constitutionnel*) only weeks before the vote (in this case, the list of the eleven qualified candidates was published on March 18). Moreover, the French election has two rounds, which creates an additional hurdle, as the meddler cannot be certain which candidates will be in the second round. This also permits voters to shift their support to another candidate and correct a wild-card result after the first round.

The media environment of the election is also more regulated in France than in the United States.[147] Paid political advertising is forbidden: during the six months prior to the election, the Electoral Code prohibits “the use, for the purpose of election propaganda, of any commercial advertising in the press or any means of audiovisual communication” (Article L. 52-1). Paid advertisements cannot contain “references, verbal or visual, to candidates or election-related issues.” Official political ads, of equal duration, can be aired for free on national TV and radio stations during the official campaign period. Airtime allocated to politicians and political parties in broadcast media is also regulated: starting on February 1, 2017, the French media regulatory authority (CSA) began implementing the equal-time rule, counting the amount of speaking time and airtime allocated to each candidate to ensure fairness and equitable treatment. The law also requires media that publish opinion polls to explain how they were conducted. Publication of or commentary on any pre-election opinion poll is banned on Election Day and the day before. There is an election silence, i.e. a “media blackout,” starting at midnight the day before the election until the polls close, a period during which “the dissemination to the public, by electronic means, of any message that constitutes election propaganda is prohibited” (Article L. 49).

“this success was due to a combination of structural factors, luck, and the effective anticipation and reaction”

Second, the French media environment was (then) relatively robust. There is a strong tradition of serious journalism, the population consumes mostly mainstream media sources, social networks penetration is lower, and tabloid-style outlets and “alternative” websites are less popular than they are in the United States

[146] *Ibid*.

[147] For a comparison with other OSCE countries, see Davor Glavaš, *Political advertising and media campaign during the pre-election period: A Comparative Study*, commissioned by the OSCE Mission to Montenegro, May/July 2017.

and the United Kingdom. In January 2017, when the disinformation campaign started, the internet penetration rate was lower in France than in the United States, Germany, Canada, or the United Kingdom.[148] Social media penetration was particularly low (56 percent of the population, compared with 64 percent in the United Kingdom and 66 percent in the United States), as is time spent daily on social media (one hour and twenty-three minutes on average in France, 1:48 in the United Kingdom, and 2:06 in the United States). French readers are also more critical: their overall trust in news media is lower than in most countries (30 percent in France, 38 percent in the United States, 43 percent in the United Kingdom).[149] They clearly do not trust social networks as news sources: a survey showed that while 75 percent of the population trusts news from "traditional" media, only 25 percent trusts news found on social networks.[150]

An Oxford University study of more than eight hundred thousand tweets found that while in the US election "25.9 percent of all the links being shared led to professional news content and 3.4 percent of the links led to content from traditional political parties, government agencies, or other experts," in the French election it was 46.7 percent and 15.7 percent, respectively. The study concluded that "French voters are sharing better quality information than what many US voters shared, and almost as much quality news and information as German users share."[151] Another study based on the eight hundred most-visited websites and almost eight million links shared in the run-up to the presidential election (November 2016–April 2017) showed that "traditional media and campaign sources make up 56% of all shared links in the public discourse" and only "24% of the shared citations come from sources which challenge traditional media narratives."[152] It must be said, however, that what was true in 2017 may no longer be true, as the yellow vests (*gilets jaunes*) movement both revealed and boosted the growing role of "alternative" and conspiratorial media in France.

Moreover, in the two years before 2017, two specific episodes contributed to reinforce the robustness of the French media and opinion. On the one hand, the 2015 TV5Monde cyberattack, which was pretty serious. "We were a couple of hours from having the whole station gone for good," remembered Yves Bigot, the director-general of TV5Monde.[153] It served as a wake-up call for most of the French media. On the other hand, the online jihadist propaganda, especially as France suffered regular terrorist attacks on its soil, marking for many the end of innocence and the beginning of distrust towards the digital platforms. Right after the 2015 terrorist attacks, the French government launched a public campaign to fight jihadist propaganda (stop-djihadisme.gouv.fr). Those two episodes contributed to build a general awareness of risks of cyberattack and information manipulation among the French media and opinion in the 2015-2017 period, that proved useful when came the "Macron Leaks" operation.

"French voters are sharing better quality information than what many US voters shared"

Third, Cartesianism also plays a role. Rationality, critical thinking, and healthy skepticism are parts of the French DNA and are encouraged as early as primary school and throughout professional life. Skepticism itself is a double-edged sword, as it is also a quality encouraged by the so-called "alternative" media, which rely precisely on their users' habit to doubt "official" versions of things. RT's motto is "Question more." Skepticism in itself is of neutral value; it serves both information manipulation and information defense. In reference to RT's motto, the EU East StratCom Task Force's motto is "Don't be deceived: question even more." Skepticism should never be an end in and of itself. According to French philosopher René Descartes, the "hyperbolic doubt" is only methodological, a means to reach knowledge, and knowledge is based on reason. The unhealthy skepticism on which disinformation relies, especially in its conspiratorial extension, is a Pavlovian

[148] Simon Kemp, *Digital in 2017 Global Overview, We are social and Hootsuite*, January 2017, 28 and 41.

[149] Reuters Institute, *Digital News Report 2017*, 20, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0.pdf.

[150] "3 Français sur 4 se méfient des informations diffusées via les réseaux sociaux," *La Tribune*, December 18, 2017, https://www.latribune.fr/technos-medias/3-francais-sur-4-se-mefient-des-informations-sur-les-reseaux-sociaux-762159.html.

[151] Philip N. Howard *et al.*, *Junk News and Bots during the French Presidential Election: What Are French Voters Sharing Over Twitter? Data Memo 2017.3, Oxford University Project on Computational Propaganda*, April 22, 2017, 5. In the German sample, results are 44.9% and 13.7% respectively.

[152] *2017 French Election Social Media Landscape: The Role and Impact of Non-Traditional Publishers in the French Elections 2017, Bakamo*, April 19, 2017, 7.

[153] Gordon Corera, "How France's TV5 was almost destroyed by 'Russian hackers'", BBC News, 10 October 2016.

reflex to doubt anything “official.” The healthy skepticism that runs through the French education system is more a rationalist reflex to doubt anything not demonstrated. This played a role in the resistance of the French population to the “Macron Leaks” operation.

2. LUCK

In this story, as in any success story, luck played a role. The Macron team was lucky that the attackers were sloppy and made a number of mistakes. The attackers were emboldened by recent successes (the EU-Ukraine referendum in the Netherlands, Brexit, and the US elections). They also had reasons to believe that France was going to be an easy target: the popularity of the National Front, the fact that most of the main candidates were pro-Russia (of the four main contenders, Macron was the only one not in favor of lifting European sanctions), and terrorist attacks that had provoked Islamophobia and division. Furthermore, the attackers came unprepared, lacking sufficient knowledge of their target state. Consider a comparison to Germany: “the German battlespace has been studied much more by both the alt-right and the Kremlin for years now. It’s been much more carefully prepared.”[154]

> *“The unhealthy skepticism on which disinformation relies, especially in its conspiratorial extension, is a Pavlovian reflex to doubt anything ‘official.’”*

And, finally, like most people, the attackers simply did not anticipate that Macron would have a viable shot at the presidency. Until the end of January 2017, polls predicted that the second round would be Fillon against Le Pen—either way a win-win for the Russians, who just had to stand back and wait. Macron was not a front-runner until early February, when he became a last-minute target, but “the shorter schedule limited opportunities for hackers to infiltrate the campaign.”[155] That is an important difference with the US case, where Hillary Clinton was a long-planned target. “Until [the relatively pro-Russia, center-right contender François] Fillon began to suffer as a candidate, the Kremlin disinformation machine in France was basically running in neutral …then there was this rush to try and discredit Macron,”[156] Nimmo said. Not only did the attackers lack sufficient time to find dirt on him, but he was also “too young to be dirty”[157]: his short track record meant that there was not much to dig up. “This is a nightmare scenario for an intelligence agency on a deadline. Caught off guard by a fast moving, clean politician with no time to locate any dark secrets or prepare a scandal.”[158]

The attackers who tried for months to collect incriminating information on Macron must have been disappointed to find nothing in the emails and other documents they stole. They had to taint the leak, modifying the content to make it look more scandalous, but they did it so clumsily that it was unconvincing, as they probably realized. Their last chance was not the content, where there was nothing to find, but the package: not what was in the leak, but the fact that there was a leak. Hence the combination of timing (at the last moment, hours before the electoral silence) and size (the package was artificially inflated by the addition of unrelated material to make the total size bigger): the leak was too large to be analyzed thoroughly in the available time, i.e. before the vote. The bet was that people would think that there “must” be something and would be inclined to believe the trolls all over the digital platforms who pretended to have found really scandalous stories in the leak. That would have been, indeed, a “clever approach to creating something from nothing.”[159]

Except that it did not work, due to a number of mistakes. First, the saboteurs overestimated their ability to shock and mobilize online communities, and they underestimated the resistance and the intelligence of the mainstream media. Above all, they did not expect the Macron campaign staff to react—let alone react so well. They also overestimated people’s interest in a leak that revealed nothing. As it became obvious that the thousands of emails were, at best, boring and, at worst, ludicrous, the public lost interest.

Second, launching the offensive just hours before the electoral-silence period was a double-edged sword.

[154] Ben Nimmo, interviewed in Sam Jones, “Flawed Macron hack provides lessons for both sides,” *The Financial Times*, May 9, 2017.

[155] Isabella Hansen and Darren J. Lim, “Doxing democracy: influencing elections via cyber voter interference,” *Contemporary Politics* (2018), 14.

[156] Nimmo, interviewed in Sam Jones, “Flawed Macron hack.”

[157] thaddeus t. grugq, “A Last Minute Influence Op by Data DDoS,” *Medium.com*, May 6, 2017.

[158] *Ibid*.

[159] *Ibid*.

While it rendered Macron unable to defend himself and the mainstream media unable to cast a critical eye on the leaks, it also left provocateurs insufficient time to spread the information. Even Assange acknowledged that “the Macron leaks came too late to have an impact on the elections.”[160] The timing also rendered the entire revelation highly suspicious.

Third, some of the fake documents were so absurd and clumsily drafted that the whole episode seemed amateurish. The “Macron Gate” documents were obviously forged and, in the words of Mahjoubi, “amateurish fake news.”[161] Some of the leaked emails, like those mentioning masturbation or cocaine, were too exaggerated to be believable.

Fourth, the attack suffered from cultural clumsiness. That is best illustrated in the attempt to spread the rumor that Macron is gay, which may have been scandalous for a Russian or an American politician but hardly for a French one. Bertrand Delanoë, for example, revealed he was gay in 1998 and was elected mayor of Paris three years later, then reelected for a total stay of thirteen years in office. The French do not really care about the private lives of their leaders. Hollande, the incumbent president, had an affair with an actress; François Mitterrand, who was president between 1981 and 1995, even had a daughter with his mistress, whose existence was revealed at the end of his presidency without causing much indignation. Playing the “morality” card to hurt a French politician—even more so a liberal politician whose electorate is by definition progressive—by spreading rumors that he is gay and/or unfaithful is doomed to fail and only reveals the conservatism of the attackers.

> *“Paris benefited from the mistakes it witnessed during the American presidential campaign”*

Fifth, and more generally, cultural clumsiness in this operation was caused—and revealed—by the language itself. Most of the catalyst accounts (and bots) were in English because the leaks were first spread by the American alt-right community. However, this posed two kinds of problems. On the one hand, this was not an effective means of penetrating a foreign population known to have poor foreign-language skills. As noted by Emilio Ferrara, the key participants in the Macron leaks were mainly “in the English-speaking American user base.”[162] These users’ prior interests included steadfast support for Trump and Republican views, as well as more extreme, alt-right narratives. This leads to one possible explanation for the limited success of the disinformation campaign: voters did not significantly engage with or discuss the leaked documents. After analyzing a dataset of seventeen million Twitter posts between April 27 and May 7, Ferrara concluded that “the reasons of scarce success of this campaign [are that] the users who engaged with MacronLeaks are mostly foreigners with preexisting interest in alt-right topics and alternative news media, rather than French users with diverse political views.”[163]

On the other hand, English-language interference could have been counterproductive in a country where a significant part of the population is either hostile to or skeptical of American actions. “Two of the biggest characteristics of French nationalists are resistance to US dominance and resistance to English-language words being used in French,” Nimmo said. “So the effect of a hashtag campaign originating among right-wing American accounts—MacronLeaks and not even FuiteMacron—was horrendously ham-fisted.”[164]

For all these reasons, France was fortunate in that smarter attackers under the same conditions could have had a much more severe impact. But some people make better use of their good luck than others. In this instance, the operation’s failure should also be attributed to preparation, swift reaction, and coordination by the Macron campaign staff, the government, and civil society.

3. ANTICIPATION

Lesson 1: Learn from others

France had the advantage of being targeted after cyberattacks and disinformation campaigns in the Netherlands, the United Kingdom, and the United States. All of these precedents, especially the American one, were useful in raising awareness. The 2016 US presidential campaign was a game-changer: before

[160] Julian Assange, interviewed by Michael Sontheimer and Joerg Schindler, “WikiLeaks Will Always Be the Bad Boy,” *Der Spiegel*, May 19, 2017.

[161] Quoted in Lecadre, Albertini, and Guiton, “Compte aux Bahamas.”

[162] Ferrara, “Disinformation and Social Bot Operations.”

[163] *Ibid*.

[164] Nimmo, interviewed in Jones, “Flawed Macron hack.”

Admiral Michael S. Rogers, the National Security Agency director, told Congress in May 2017, “If you take a look at the French election … we had become aware of Russian activity. We had talked to our French counterparts prior to the public announcements of the events publicly attributed this past weekend and gave them a heads-up: ‘Look, we’re watching the Russians, we’re seeing them penetrate some of your infrastructure.’” *Photo Credit: C-Span.org*

the election, awareness of disinformation was mostly limited to the Baltic and Central European states. Since then, large Western European states have learned that they are also vulnerable and should be concerned. In other words, the US case had an immunizing effect. Mika Aaltola compared election meddling in the US, French, and German elections and concluded that “the evidence points to a downstream effect whereby external meddling becomes less effective in subsequent elections when its tactics and impact are widely publicized after one notable case. As the immunity strengthens down the stream of a series of elections, the successful utilization of the same tactic can even lead to opposite and more detrimental strategic results from the perspective of the illicit actor.”[165]

Paris benefited from the mistakes it witnessed during the American presidential campaign: the disdain and neglect for disinformation campaigns, a reluctance to address and frame the hacking of the DNC, and a delayed response by the government. It also benefited from operational cooperation with the US authorities. In January 2017, then-Defense Minister Jean-Yves Le Drian acknowledged that “our services have the necessary exchanges on this subject, if only to draw lessons for the future.”[166] Also, during its presidential campaign, France was warned by the United States that it “had become aware of Russian activity.” Admiral Michael S. Rogers, the National Security Agency director, told Congress in May 2017, “If you take a look at the French election … we had become aware of Russian activity. We had talked to our French counterparts prior to the public announcements of the events publicly attributed this past weekend and gave them a heads-up: ‘Look, we’re watching the Russians, we’re seeing them penetrate some of your infrastructure.’”[167]

[165] Mika Aaltola, *Democracy’s Eleventh Hour: Safeguarding Democratic Elections Against Cyber-Enabled Autocratic Meddling, Finnish Institute of International Affairs Briefing Paper 226*, November 2017, 6-7.

[166] Jean-Yves Le Drian (minister of defense), interviewed in *Le Journal du Dimanche*, January 8, 2017.

[167] “Admiral Rogers Says Intel Community Warned of Russian Hacking Ahead of Macron Leak,” C-SPAN, May 9, 2017, https://www.c-span.org/video/?c4668917/admiral-rogers-intel-community-warned-russian-hacking-ahead-macron-leak

The Conseil d’Etat, where the CNCCEP was installed. *Photo Credit: Wikimedia Commons.*

Lesson 2: Use the right administrative tools

The Obama administration did not intervene in the electoral process even when the process was under siege because it did not want to give the impression of advantaging the Democratic candidate (and because it was confident that Clinton would win anyway). However, the French case shows that a government can intervene and take measures, provided that these measures are carried out by administrative, independent, non-political authorities. In France, these authorities provided technically sophisticated and politically neutral expertise in order to guarantee the integrity of the electoral process from start to finish.

Three bodies played a particularly crucial role. First, the Constitutional Council (Conseil constitutionnel) which, by law, remains the electoral judge and guarantor of the integrity of the vote: according to Article 58 of the constitution, it “shall ensure the proper conduct of the election of the President of the Republic.” It set up a dedicated website (presidentielle2017.conseil-constitutionnel.fr), which received 1.3 million visitors.[168]

Second, the National Commission for the Control of the Electoral Campaign for the Presidential Election (CNCCEP), a temporary body set up two months before the presidential election to serve as a campaign watchdog. Physically installed at the Council of State (Conseil d’Etat), its role is to ensure respect for the principles of equality (among the candidates) and neutrality (of public services) during the campaign.

Third, there is the National Cybersecurity Agency (ANSSI), within the Secretariat-General for National Defence and Security (SGDSN), an interministerial organ under the French Prime Minister. Its general role is “to foster a coordinated, ambitious, pro-active response to cybersecurity issues in France.”[169] During the 2017 presidential election, the challenge was to “ensure the integrity and accessibility of the electoral process while remaining neutral with respect to it, ensure its transparency to maintain confidence in the election while ensuring the confidentiality of votes, and ensure security while maintaining the accessibility of systems.”[170] The SGDSN tasked ANSSI with the online monitoring during the electoral campaign and asked the agency to report any suspicious activity to the CNCCEP and the Constitutional Council.[171] ANSSI was also authorized to assist political parties by providing politically neutral, technical expertise. This was a new task for the agency.

Moreover, these bodies maintained open channels of communication with one another. The ministries and authorities involved in national security regularly met with the president within the Defense and National Security Council (Conseil de défense et de sécurité nationale) to exchange information, study the problem, and coordinate potential responses.

[168] Conseil constitutionnel, *Annual Report 2017*, 8.

[169] ANSSI website (ssi.gouv.fr), “A Word from the Director General.”

[170] ANSSI, *Rapport d’activité 2017*, 17.

[171] Hearing of Louis Gautier (SGDSN) at the National Assembly, 21 February 2018, in *Rapport fait au nom de la commission de la défense nationale et des forces armées sur le projet de loi (n°659) relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense*, http://www.assemblee-nationale.fr/15/rapports/r0765-tII.asp

Lesson 3: Raise awareness

At the end of the summer 2016, the SGDSN and ANSSI alerted the political parties and candidates of the risk of cyberattacks and disinformation during the presidential campaign. On October 26, 2016, ANSSI organized a workshop on cybersecurity, open to all political parties represented at the French and European parliaments. Its aim was to draw lessons from the 2016 American presidential election, to evaluate the risks in the context of the 2017 French presidential election, and to expose good practices.[172] Every political party apart from the National Front participated. ANSSI also provided campaign staff with the tools to monitor and detect suspicious activity in candidates’ information systems (including denial-of-service, or DOS, attacks, unusual activity, and intrusions). With more sophisticated systems to monitor risk, campaign staff were able to better react to and anticipate attacks, as well as to develop adequate responses to security breaches.

During the campaign, in early February 2017, ANSSI visited the Macron campaign headquarters to warn them. “Officially, it was ANSSI. But behind them, it was obviously the DGSE [the French external intelligence agency]. They told us that we were being watched, that there was a risk of piracy and that we had to be careful with Telegram, which is a Russian app,” one of Macron’s close advisers recalled.[173] After the meeting, the campaign staff switched from Telegram to WhatsApp. “We had the choice between the KGB and the NSA, we chose the NSA,” quipped Ismaël Emelien, Macron’s adviser on communication and strategic issues who later became special adviser to the president.[174]

If ANSSI was instrumental in raising awareness, the role of civil society, in particular journalists themselves, should also be highlighted. One experiment was particularly interesting: CrossCheck, a collaborative journalism project powered by the First Draft coalition and supported by the Google News Lab. Over ten weeks, between February and May 2017, it gathered more than one-hundred journalists from thirty-seven French newsrooms in order to fact-check information during the presidential election.[175]

Lesson 4: Show resolve and determination

In its 2015 French National Cyber Security Strategy, the prime minister’s office warned that disinformation and propaganda could be treated as an attack on French soil:

> 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 purposes of disinformation and spreading propaganda to French citizens, in particular the youngest 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.[176]

From the start of the electoral campaign, the French government signaled—both publicly and through more discreet, diplomatic channel—its determination to prevent, detect, and, if necessary, respond to foreign interference. In an important speech on cyberdefense in December 2016, Jean-Yves Le Drian, the defense minister, announced the creation of a cyber command composed of 2,600 “cyber fighters.”[177] A few weeks later, he said in an interview 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. This could be through our cyber arsenal but also by conventional armed means.”[178]

One month later, when En Marche! announced that it was the target of an orchestrated attack, the presidency said in a press release that Hollande had requested the Defense and National Security Council to present “the specific measures of vigilance and protection, including in the cyber domain, taken during the electoral campaign.”[179] What is significant is not the news itself—these specific measures were not made public—but the signal sent by showing the will to say publicly that specific measures were requested.

The same day, the foreign minister told parliament, “France will not tolerate any interference in its electoral process, no more from Russia than from any other state. … [We must] make the limits clearly known to

[172] *Ibid*.

[173] Quoted in Nathalie Raulin and Guillaume Gendron, “Piratage : l’équipe Macron sur le pont,” *Libération*, August 10, 2017.

[174] *Ibid*.

[175] Nikos Smyrnaios, Sophie Chauvet, and Emmanuel Marty, *The Impact of CrossCheck on Journalists & the Audience*, November 2017.

[176] *French National Cyber Security Strategy, Office of the Prime Minister*, 2015, 20.

[177] Jean-Yves Le Drian (Minister of Defense), Speech on Cyberdefense, Bruz, December 12, 2016.

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

[179] “Présidentielle: Hollande demande des mesures contre les cyberattaques,” *L’Express*, February 15, 2017, https://tinyurl.com/y4x4uuod.

those who would be tempted to undermine this principle of non-interference and we must do so clearly, including by taking retaliatory measures where necessary, because no foreign state can influence the choice of the French people, no foreign state can choose the future president of the Republic.”[180] A similar message was conveyed privately by the minister to his Russian counterpart and by Hollande to Putin.

“Facebook suspended seventy thousand accounts. It had never before taken such a drastic measure”

Drawing clear red lines and showing the determination to respond when those lines are crossed helped France to discourage foreign disinformation campaigns and laid the groundwork for a swift and firm response. US Senate Democrats, drawing lessons from the French elections in their January 2018 report for the Foreign Relations Committee, concluded that “direct diplomatic engagement clearly pointing to malicious actors and the consequences of their actions can act as a deterrent.”[181] “Deterrent” may be too strong a word, as these precautions obviously were not enough to deter the attackers behind the Macron leaks, but, given the amateurism of the attack, it can safely be assumed that the foreign power behind it exercised restraint in the face of the hard stance taken by the French authorities. “That [the leaks] happened one hour before the end of the official campaign proves in a certain way that Putin did not want to destabilize the campaign. But he wanted us to know that he could have done it,” argued one of Macron’s collaborators.[182]

Later, in February 2018, the Macron administration published The French Strategic Review of Cyber Defense*,* which affirmed France’s commitment to the work of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.[183] It emphasized the obligation for other states to assist victim states, especially if an attack passes through their territory, irrespective of the source of the attack. This document is both an attempt to free France from the attribution dilemma and a demand for international solidarity, even before its investigation into the election interference has concluded.

Lesson 5: Take (technical) precautions

ANSSI heightened security at every step of the electoral process in order to ensure the integrity of the vote. This vigilance had durable effects on subsequent elections. For example, the head of ANSSI told parliament that he was “personally” opposed to voting machines and electronic voting.[184] In France, electronic voting is permitted only for overseas voters and only in legislative and consular elections: it was not an issue for the presidential election *per se*. However, this vigilance during the presidential campaign had an indirect effect on the following legislative election (June 11 and 18, 2017): despite the unpopularity of the measure, the Foreign Ministry followed ANSSI’s recommendation. On March 6, 2017, the government announced the end of electronic voting for citizens abroad because of the “extremely high risk” of cyberattacks.[185]

Lesson 6: Put pressure on digital platforms

Ten days before the vote, Facebook announced it “[had taken] action against over 30,000 fake accounts” in France.[186] Company officials later revealed to congressional committee members and staff that the number of suspended Facebook accounts was actually seventy thousand.[187] Facebook had never before taken such a drastic measure. The same day, Facebook published full-page ads in German newspapers in order to raise public awareness of the “fake news” issue. The weekend of the final vote in France, several accounts were suspended by Facebook and Twitter. Because most of them were in the “fachosphere,” the far-right online community, their activists denounced a major censorship operation

[180] Untersinger, “Cyberattaques.”

[181] Committee on Foreign Relations, *Putin’s Asymmetric Assault on Democracy in Russia and Europe: Implications for US National Security*, S. Rep. 115-21, at 125 (2018) (Minority Staff Rep.).

[182] Quoted in Raulin and Gendron, “Piratage.”

[183] See François Delerue and Aude Géry, “France’s Cyberdefense Strategic Review and International Law,” *Lawfare*, March 23, 2018 and Boris Toucas, “With its new ‘White Book,’ France looks to become a world-class player in cyber space,” *War on the Rocks*, March 29, 2018.

[184] Assemblée nationale, comments made by Guillaume Poupard, January 18, 2017, http://www.assemblee-nationale.fr/14/cr-cloi/16-17/c1617040.asp..

[185] ANSSI, *Rapport d’activité 2017*, 18.

[186] Facebook, “Improvements in protecting the integrity of activity on Facebook,” April 12, 2017, https://www.facebook.com/notes/facebook-security/improvements-in-protecting-the-integrity-of-activity-on-facebook/10154323366590766/

[187] Menn, “Exclusive: Russia used Facebook”.

(#FacebookGate, #TwitterGate). However, not only the numbers were exaggerated in a classic victimization, to make it look like some kind of organized political censorship, but the digital platforms were simply implementing the “normal process” of moderating “false accounts”[188]—and it was apparently the case that such false accounts were more numerous on the far-right side. These important steps are the result of growing pressure, by both states and the public, on digital platforms—the principal medium for the spread of disinformation.

4. REACTION

Lesson 7: Make all hacking attempts public

Throughout the campaign, the En Marche! team communicated openly and extensively about its vulnerability to hacking and, soon after, about the hacking itself, acknowledging that their computer systems had been hacked. They communicated internally to raise awareness among the Macron campaign. “Every week we send to the team screen captures of all the phishing addresses we have found during the week,” Mahjoubi explained.[189] And they communicated externally by making all hacking attempts against them public, generating awareness among the population and the authorities.

When the Macron leaks occurred*,* En Marche! reacted in a matter of hours but was careful neither to overreact nor to violate the electoral silence. “Overreacting would have been inopportune and risky,” one of the movement’s lawyers explained. “Inopportune because it would have given exaggerated importance to a technique, certainly without precedent, but whose echo, outside of Twitter, remained weak. Risky because the candidate would have committed a violation of the electoral law. … In the small Parisian milieu addicted to Twitter, it was a huge thing, but elsewhere?”[190]

At 11:56 p.m. on Friday, May 5, only hours after the documents were dumped online and four minutes before the electoral silence went into effect, the Macron campaign issued a press release stating:

> The movement has been the victim of a massive and coordinated hacking operation giving rise tonight to the dissemination on social networks of internal information of various kinds (e-mails, accounting documents, contracts, etc.). The files, which are circulating, were obtained a few weeks ago from a hack of the professional and personal email accounts of several staff members of the movement. Those who circulate these documents have added many fake documents to the collection of authentic ones in order to sow doubt and disinformation. By intervening in the last hour of the official campaign, this operation is clearly a matter of democratic destabilization, as was already witnessed in the United States during the last presidential campaign.[191]

Lesson 8: Gain control over the leaked information[192]

Among the leaked data were real emails and forgeries. After a year of investigation, a journalist estimated that only around 80 percent of the dump was genuine.[193] Some fake emails were so obvious that they actually helped the Macron team. “That allowed us to pass off real emails as fakes, such as one email, which was authentic, in which a manager writes, ‘We’ll have to lay off as many employees as we can after May 5,’” one of Macron’s colleagues later explained.[194]

The campaign staff went even a step further: as the hacks could not be avoided, the team focused on slowing down the hackers by inundating them with false information and setting traps. “You can flood the emails of your employees with several passwords and log-ins, real, fake, so that the [hackers] spend a lot of time trying to understand them,” Mahjoubi explained.[195] Therefore, the leak contained documents forged by the campaign team itself: “information that we ourselves had sent in counter-retaliation for phishing attempts!”[196] This

[188] Vincent Coquaz, “La fachosphère ‘censurée’ sur Twitter et Facebook avant le second tour ?”, *Libération*, 9 May 2017.

[189] Dickey, “Fighting Back Against Putin’s Hackers.”

[190] Quoted in Raulin and Gendron, “Piratage.”

[191] “Communiqué de presse - En Marche a été victime d’une action de piratage massive et coordonnée,” May 5, 2017 https://en-marche.fr/articles/communiques/communique-presse-piratage.

[192] In previous publications, I titled “Beat hackers at their own game.” However, as Joel Harding noted, “This is not about beating hackers, it is about gaining a modicum of control over the information when it is leaked” (his blog toinformistoinfluence.com, June 25, 2018)**.**

[193] Antton Rouget, quoted in Jacques Pezet, “Was wurde aus den Macron-Leaks?” *Correctiv*, May 7, 2018.

[194] Raulin and Gendron, “Piratage.”

[195] Mahjoubi, interviewed in Raphaël Bloch, “MacronLeaks: comment En Marche a anticipé les piratages,” *Les Echos*, May 10, 2017.

[196] Mahjoubi, interviewed in Antoine Bayet, “Macronleaks: le responsable de la campagne numérique d’En marche! accuse les ‘supports’ du Front national,” France Info, May 8, 2017.

diversionary tactic, which involves creating fakes to confuse attackers with irrelevant and even deliberately ludicrous information, is called “cyber-” or “digital blurring.” “We created false accounts, with false content, as traps. We did this massively, to create the obligation for them [the hackers] to verify, to determine whether it was a real account. … During all their attacks we put in phony documents. And that forced them to waste time.”[197]

> *“This diversionary tactic, which involves creating fakes to confuse attackers with irrelevant and even deliberately ludicrous information, is called “cyber-” or “digital blurring.”*

Some of the fakes looked real, others not: they were intentionally ridiculous, with even references to French popular culture that indicate they were made in-house. One obvious example was an email supposedly originating from Macron’s director of general affairs to a “David Teubey” and a “Greg Latache,” both with en-marche.fr email addresses, with “bill.trumendous@cia.gov” in cc, about a plan to scrap Airbus A400M military aircraft after the election to replace them with Boeing models. That was a honey-pot story for conspiracy theorists, who see the CIA everywhere and spread claims that Macron is an American puppet. However, “David Teubey” (last name is “stupid” in *verlan*, an argot inverting syllables) and “Greg Latache” (last name means “the stain,” a colloquial term for someone who is incompetent and useless) are characters invented by two French humorists more than a decade ago, and Bill Trumendous (Tremendous) is the CIA agent in the French spy comedy movie *OSS 117: Lost in Rio*. Therefore, this fake email appears to be the Macron team’s attempt to humorously trap the attackers, discrediting both them and the entire leak, and have fun in the process.

Another obviously fake email also allegedly written by the director of general affairs, included statements such as “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.”[198]

In reacting this way, the Macron team’s strategy was “to preemptively degrade the value that might be derived from leaked campaign documents”[199] and to place the burden of proof back onto the attackers. The Macron campaign did not have to justify potentially compromising information contained in the leaks; rather, the hackers had to justify stealing and leaking information that seemed, at best, useless and, at worst, false or misleading. People hence doubted the authenticity of the leaks, and the hackers saw “the material that they assumed would be politically explosive for Mr. Macron’s electoral prospects explode in their own faces.”[200]

Lesson 9: Stay focused and strike back

The purpose of these attacks “is to unfocus us,” Mahjoubi said. “My role in this campaign is to make sure our message goes through.”[201] In order to do so, the campaign adopted both positive and negative approaches: it continued hammering its political program home and responded to the disinformation efforts. The forceful presence of Macron’s young—most were under twenty-five years old—campaign staff on social media enabled them to systematically respond to posts or comments that mentioned the “Macron Leaks.”

Lesson 10: Use humor

In certain instances (such as those mentioned in lessons 8 and 9), the campaign’s injection of humor and irony into its responses boosted its visibility and popularity across different platforms.

[197] Mahjoubi, interviewed in Adam Nossiter, David E. Sanger, and Nicole Perlroth, “Hackers Came, but the French Were Prepared,” *The New York Times*, May 9, 2017.

[198] Josh Caplan,“Grégoire Potton, director of gen. affairs @ #EnMarche tells staff ‘baise le peuple,’ which means ‘fuck the people’ #MacronGate #MacronLeaks” Twitter Account, May 6, 2017, 7 :46 a.m. https://tinyurl.com/y22gk7n3

[199] Erik Brattberg and Tim Maurer, *Russian Election Interference: Europe’s Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, May 2018, 9, https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.

[200] Jonathan Eyal, “How France Fought Off Influence Ops in the Last Election,” *The Straits Times*, July 2, 2018, https://www.straitstimes.com/opinion/how-france-fought-off-influence-ops-in-the-last-election.

[201] Dickey, “Fighting Back Against Putin’s Hackers.”

Lesson 11: Alert law enforcement

The leak being apparently in violation of the Electoral Code, the CNCCEP referred the case to the public prosecutor’s office in Paris within a few hours of the initial dump. The prosecutor’s office opened an investigation, which was entrusted to the Information Technology Fraud Investigation Brigade of the Paris police.[202]

Lesson 12: Undermine propaganda outlets

On April 24, the day after the first round of the presidential election, Macron’s campaign confirmed that it had denied accreditation to RT.[203] Three days later, it said it had denied both RT and Sputnik accreditations to cover the rest of the campaign. The reason cited was their “systematic desire to issue fake news and false information” as well as their “spreading [of] lies methodically and systematically.”[204] Even since the election, both outlets have sometimes been banned from press conferences at the Élysée Presidential Palace and Foreign Ministry.

This measure has been controversial. It fueled the Kremlin’s narrative that France is engaging in the exact activities for which it criticizes Russia, allowing Putin to lecture France on freedom of the press—which is ironic coming from a country ranked 148th in Reporters Without Borders’ 2018 World Press Freedom Index (versus 33rd for France).

However, the decision to ban RT and Sputnik from only certain events was justified on two grounds. First, they are not genuine press outlets but rather propaganda organs. This has been the position of the European Parliament since at least November 2016. In its resolution on EU strategic communication to counteract propaganda, the European Parliament described RT and Sputnik as “pseudo news agencies.”[205] Macron expressed the same position during the campaign and most famously at a press conference with Putin at the Versailles palace, only weeks after his election. When asked why RT and Sputnik were banned from his headquarters at the end of the campaign, he responded:

> Russia Today and Sputnik were organs of influence during this campaign that repeatedly produced counterfeit truths about me and my campaign. … And it’s worrying that foreign media outlets–under the influence of some other party, whomever that may be–interfered by spreading serious untruths in the midst of a democratic campaign. And to that [behavior] I will not concede anything, nothing. … Russia Today and Sputnik have not behaved like members of the press or like journalists, but instead have behaved like organs of influence and deceitful propaganda, no more, no less.[206]

This statement made a powerful impression abroad. It signaled the determination of the new French president to tackle the disinformation issue head-on.

“There were three levels of communication: the trivial and logistical by email, the confidential on the [encrypted] apps, and the sensitive in face-to-face…”

Second, attendance at these press conferences is by invitation only, so there is no need for French institutions to justify excluding these news outlets. As long as RT and Sputnik are allowed to operate in the country, which they are, their rights have not been infringed, a position shared by Ambassador Daniel Fried: “rather than ban RT, I think labeling them—as we have—as a foreign agent or doing what Macron did is the way to go. They ought—they can be anathematized without being banned.”[207]

Two years later, that position is unchanged: on February 15, 2019, the campaign manager of LREM confirmed

[202] Brigade d’enquêtes sur les fraudes aux technologies de l’information (BEFTI).

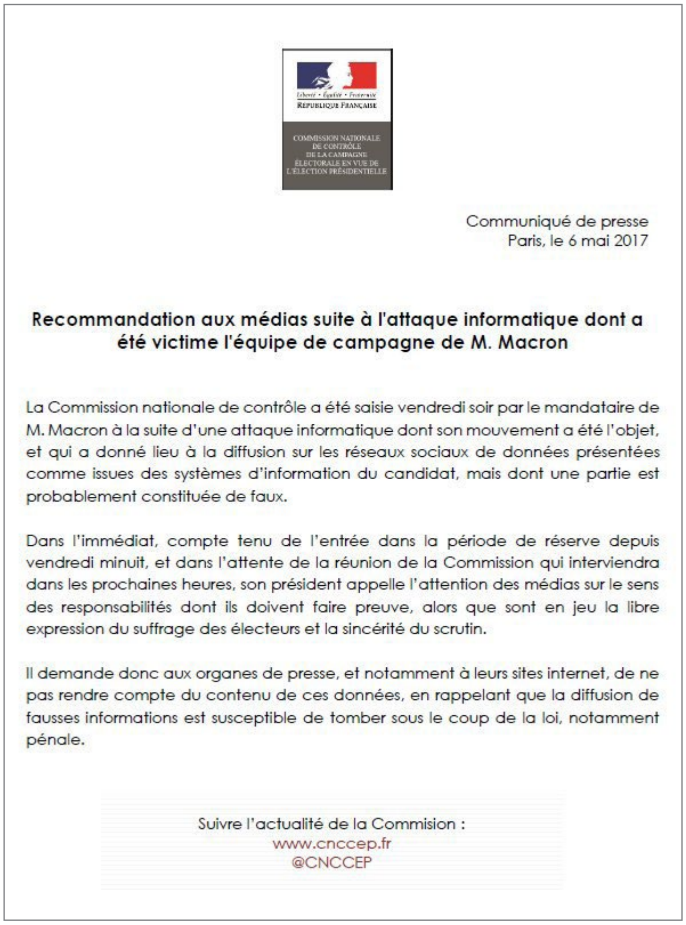
[203] Christopher Dickey, “Amid Hacking Threat, Macron Campaign Blacklists Putin’s TV Network,” *The Daily Beast*, April 24, 2017, https://www.thedailybeast.com/emmanuel-macrons-campaign-blacklists-rt-putins-tv-network.

[204] Macron spokesman in Andrew Osborn and Richard Balmforth, “Macron camp bars Russian news outlets, angers Moscow,” Reuters, April 27, 2017, https://www.reuters.com/article/us-france-election-macron-russia/macron-camp-bars-russian-news-outlets-angers-moscow-idUSKBN17T2GB.

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

[206] Emmanuel Macron, Press Conference with Vladimir Putin, Versailles, May 29, 2017, my translation. See James McAuley, “French President Macron blasts Russian state-owned media as ‘propaganda,’” *The Washington Post*, May 2, 2017, https://www.washingtonpost.com/world/europe/french-president-macron-blasts-russian-state-run-media-as-propaganda/2017/05/29/4e758308-4479-11e7-8de1-cec59a9bf4b1_story.html?utm_term=.ae068b76dfe9.

[207] Ambassador Daniel Fried at the Atlantic Council #DisinfoWeek Madrid 2019, March 8, 2019.



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

COMMISSION NATIONALE
DE CONTRÔLE
DE LA CAMPAGNE
ÉLECTORALE EN VUE DE
L'ÉLECTION PRÉSIDENTIELLE

Communiqué de presse
Paris, le 6 mai 2017

Recommandation aux médias suite à l'attaque informatique dont a été victime l'équipe de campagne de M. Macron

La Commission nationale de contrôle a été saisie vendredi soir par le mandataire de M. Macron à la suite d'une attaque informatique dont son mouvement a été l'objet, et qui a donné lieu à la diffusion sur les réseaux sociaux de données présentées comme issues des systèmes d'information du candidat, mais dont une partie est probablement constituée de faux.

Dans l'immédiat, compte tenu de l'entrée dans la période de réserve depuis vendredi minuit, et dans l'attente de la réunion de la Commission qui interviendra dans les prochaines heures, son président appelle l'attention des médias sur le sens des responsabilités dont ils doivent faire preuve, alors que sont en jeu la libre expression du suffrage des électeurs et la sincérité du scrutin.

Il demande donc aux organes de presse, et notamment à leurs sites internet, de ne pas rendre compte du contenu de ces données, en rappelant que la diffusion de fausses informations est susceptible de tomber sous le coup de la loi, notamment pénale.

Suivre l'actualité de la Commission :
www.cnccep.fr
@CNCCEP

CNCCEP Press Release.

that they “will not accredit Russia Today or Sputnik to cover our campaign [for the European parliament election]. They are not press organs but propaganda in the service of the Kremlin. They should not be treated as media, which check or cross-reference information.”[208]

Lesson 13: Trivialize the leaked content

The En Marche! press release said that the leaked documents “reveal the normal operation of a presidential campaign.” Several media outlets used them to tell the “secret story” behind how Macron’s campaign raised almost €13 million in record time without the help of a political party or public money. However, nothing illegal was found. Overall, and apart from the fundraising method, nothing interesting was found in the leaked documents at all.[209] Numerama, a French news website specializing in digital life, analyzed the data and found it “utterly mundane … One finds memos, bills, loans for amounts that are hardly over-the-top, recommendations and other reservations, amidst, of course, exchanges that are strictly personal and private—personal notes on the rain and sunshine, a confirmation email for the publishing of a book, reservation of a table for friends, etc.”[210]

These mundanities worked in the Macron campaign’s favor: they proved that, even behind closed doors, the campaign was clean. The fact that there was nothing harmful in the leaks made the leaks themselves actually positive for Macron’s image. “It turned out to be very good in terms of communication, Emelien [Macron’s communication adviser] was happy,” one of the staff recalled.[211] Indeed the episode proved so advantageous for Macron that it triggered some inverse conspiracy theories, as “rumors started to spread that it [the leak] came from us, that all these gigabytes of docs were fake in order to make people believe we were clean.”[212]

Lesson 14: Compartmentalize communication

One reason there was nothing scandalous in the leaked emails is because Macron’s campaign staff was aware, from the beginning, of the intrinsic vulnerability of an email account. They understood that everything they wrote could one day be hacked and leaked. Therefore, a member of the team explained, “There were three levels of communication: the trivial and logistical by email, the confidential on the [encrypted] apps, and the sensitive in face-to-face. … That’s why there were not so many problematic emails in the Macron leaks. Nothing that could offend, no joke about journalists and celebrities.”[213]

Lesson 15: Call on the media to behave responsibly

At 10:00 p.m. the night of the dump, Macron’s team alerted the CSA, the French regulatory media authority. Reacting fast, at 11:30 p.m., the CSA emailed TV and radio correspondents asking them to abstain from

[208] Stéphane Séjourné, “‘Les “fake news” sont le bras armé du RN et de ses alliés’”, *Le Monde*, 15 February 2019.

[209] Marc Leplongeon *et al.*, “Présidentielle: enquête sur les MacronLeaks,” *Le Point* No. 201705, May 15, 2017, https://www.lepoint.fr/presidentielle/presidentielle-enquete-sur-les-macronleaks-15-05-2017-2127482_3121.php.

[210] Aurelien Breeden, Sewell Chan, and Nicole Perlroth, “Macron Campaign Says It Was Target of ‘Massive’ Hacking Attack,” *The New York Times*, May 5, 2017, https://www.nytimes.com/2017/05/05/world/europe/france-macron-hacking.html.

[211] Quoted in Raulin and Gendron, “Piratage.”

[212] *Ibid.*

[213] *Ibid.*

Ben Nimmo, one of the leading analysts in information defense, here at #DisinfoWeek event in Brussels, March 7-8, 2019.

disseminating any information on the election coming from the digital platforms. “The aim of this preventive action was to rapidly alert publishers against the dissemination of false news that could have an impact on the conduct of the electoral weekend,” the CSA later explained.[214]

Macron’s team also alerted the CNCCEP, the electoral commission, which issued a press release the following day. Titled “Recommendation to the media following the computer attack on Macron’s campaign team,” the press release drew “the attention of the media to what is expected of them, because the free expression of the electorate and the sincerity of the ballot are at stake.” The president of the CNCCEP asked “the media not to report on the content of this data, especially on their websites, reminding the media that the dissemination of false information is a breach of law, above all criminal law.”[215] The CSA also forwarded this message to broadcast media.[216]

> *“the CNCCEP’s call “was crucial to mitigate the magnitude of the disinformation campaign.””*

The majority of traditional media sources responded by agreeing to wait until the election was over before

[214] CSA, *Rapport sur les campagnes électorales. Election présidentielle (23 avril – 7 mai 2017), Elections législatives (11-18 juin 2017)*, Paris, April 2018, 23.

[215] Commission Nationale de Contrôle de la Campagne électorale en vue de l’Élection Présidentielle, “Recommandation aux médias suite à l’attaque informatique dont a été victime l’équipe de campagne de M. Macron” Paris, May 6, 2017, http://www.cnccep.fr/communiques/cp14.html.

[216] CSA, *Rapport sur les campagnes électorales*.

investigating and publishing the leaked documents. Several media outlets also noted the timing of the leaks and asked readers to exercise caution before responding to what might be an attempt to destabilize the presidential election. *Le Monde's* reaction, for instance, was exemplary. It published a short article on May 6 to explain its position: “Whatever the origin of the hack, the publication of these documents only two days before the second round, in the blackout period prohibiting candidates and their supporters from expressing themselves, is clearly aimed at the disruption of the electoral process underway. … If these documents contain revelations, *Le Monde* will certainly publish them after having investigated them, thereby respecting our journalistic and deontological rules and without allowing ourselves to be manipulated by anonymous actors.”[217] David Martinon, France’s ambassador for cyberdiplomacy and the digital economy, said the CNCCEP’s call “was crucial to mitigate the magnitude of the disinformation campaign.”[218]

This example recently inspired the Canadian government.[219] Unveiling its plan to fight potential election meddling in February 2019, Karina Gould, the minister of democratic institutions, said the plan was “modeled on what France has in their Conseil d’État, their kind of State Council, that kind of weighs in in elections if they see something that they think needs to be alerted to the public. And they did, in fact, when Macron leaks happened. … they kind of weighed in and told the media not to report on it, right? Because it was, they believed, from foreign interference. And so, we tried to learn from successful examples of ways of being able to block foreign interference and say, ‘How can we apply that in the Canadian context?’ ”[220]

5. STORYTELLING

The fifteen lessons in the previous pages are about the national reaction – in that case, the preparation and reaction of those involved in France. However, credit for defeating the attack goes beyond France. There was a collective and international effort to quickly analyze and publicize what was happening. Within hours after the initial dump, several analyses, for example from the UK’s Ben Nimmo, Belgium’s Nicolas Vanderbiest, and France’s Stéphanie Lamy, were able to show that the spread of #MacronLeaks was the work of the American alt-right. This proved extremely useful to orient the international media conversation, not only in the mainstream media but also on digital platforms. The main story was not about the leaked content and whether it could possibly harm Macron, but about the implication of the American alt-right in what was without a doubt some kind of influence operation against the French election. In other words, a handful of open-source researchers, by their reactivity and the quality of their analysis, helped to derail the attackers’ narrative.

Here, three additional lessons can be drawn. The first is about timing and preparedness: these analysts were able to redirect the narrative because they produced a detailed and convincing analysis in the very first few hours after the dump. And they were able to do so because they were watching these networks for months: when the names of Posobiec, Craddick, @Messsmer, and others came out, they recognized them and were able to situate them in political networks and previous information operations.

“the best way to kill a disinformation narrative is to “make a Whodunit”

The second lesson is that we need more analyses like these. What we need to defeat electoral interference is not only to create a national strategy, based on the 15 previous lessons and probably many others, but also to encourage and develop international civil society initiatives scanning the web on a permanent basis – and not just during election periods –, searching for trolls, bots, and disinformation actors, and expose their identities, methods, and networks.

Here, the Atlantic Council’s Digital Forensic Research Lab (DFRLab) is an example to follow. Their role is to identify, expose and explain deliberate falsehood online, and they excel at doing it. We need more DFRLabs, in several languages.

[217] “*Le Monde* et les documents des ‘MacronLeaks,’” *Le Monde*, May 6, 2017, https://www.lemonde.fr/politique/article/2017/05/06/le-monde-et-les-documents-des-macronleaks_5123536_823448.html

[218] David Martinon, interviewed in *News From France*, a monthly review by the French Embassy in the US, NFF-2018-06, May 4, 2018.

[219] I myself had the opportunity to present the French experience to minister Karina Gould in June 2018 in Ottawa and then to the entire Canadian government, including PM Justin Trudeau, during their cabinet retreat in Nanaimo, B.C., at the end of August 2018.

[220] Karina Gould, interviewed by Chris Hall on CBC Radio, February 2, 2019.

The third lesson is that, as Ben Nimmo convincingly explains, the best way to kill a disinformation narrative is to “make a Whodunit”. Fact-checking is not enough. What we are facing is less information warfare than “narrative warfare”. In Nimmo words, “We have the facts,” but “they have the stories.” Then we need to push other stories, deconstructing theirs by showing the sources of disinformation, “share the how, take the reader on the journey.” Not only this is more attractive than boring fact checks, but it can “actually teach [readers] the skills in advance … then it is them who is being Sherlock Holmes.”

Conclusion: The Road Ahead

Finnish researcher Mika Aaltola, who used the 2016 US presidential election as a reference case, has identified five distinct stages of election meddling: “1) using disinformation to amplify suspicions and divisions … 2) stealing sensitive and leakable data … 3) leaking the stolen data via supposed ‘hacktivists’ … 4) whitewashing the leaked data through the professional media … 5) secret colluding [between a candidate and a foreign state] in order to synchronize election efforts.”[221] The Macron leaks reached only stage three: there was a disinformation campaign, data hacking, and large-scale leaking of emails and text documents, but no whitewashing or mainstreaming. What was prevented was “information laundering,” the process by which the initial traces of meddling are “washed” from the information, stories, and narrative.[222] According to Le Drian, the former defense minister, it is “the ‘laundering’ of this counterfeit online currency of invented news, disseminated and then relayed by authorities, [that] legitimizes them in the public’s eyes.”[223] This was prevented thanks to the aforementioned countermeasures and the resilience of the French media environment. Overall, structural factors as well as an effective, responsive strategy allowed the French to mitigate the damage of the “Macron Leaks” operation. “While French security officials made admirable efforts to protect against interference, what is more remarkable are the significant preparations made at the party level, in particular by En Marche,” Erik Brattberg and Tim Maurer rightly observed. [224]

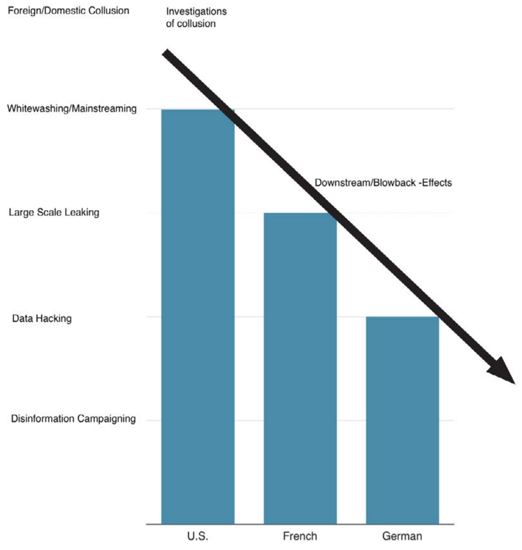


Figure 1. The five stages of election meddling in the three elections

Finnish researcher Mika Aaltola, who used the 2016 US presidential election as a reference case, has identified five distinct stages of election meddling *Source: https://www.fiia.fi/wp-content/uploads/2017/11/bp226_democracys_eleventh_hour.pdf*

Such congratulations are well-deserved, but there are at least three reasons why France should not rest on its laurels. First, this is a case of election interference, a quite specific type of information manipulation. Some of the factors that helped France in this case, like the media blackout (electoral silence), the intervention of the electoral commission (CNCCEP), or even raising awareness for most, if not all, of the political parties, are specific to elections: they will be of no help in other situations. As well as being a staple of upcoming political campaigns information manipulation is used between elections to sow mistrust and division within societies. We must insist that this is a daily threat, not one reemerging every two years or so. Focusing on elections, as governments usually do, is a good opportunity to interest politicians and the people because no one opposes protecting the integrity of the ballot. However, measures taken should certainly not be limited to electoral periods. Recent examples of disinformation campaigns, surfing on the yellow vest movement,[225] the UN Migration Pact,[226] the Aachen Treaty,[227] or even the Notre Dame cathedral fire,[228] are useful reminders that France’s adversaries would use any opportunity, anytime, to divide and spread doubt, confusion and conspiracies.

[221] Aaltola, *Democracy’s Eleventh Hour*.

[222] Boris Toucas, *Exploring the Information-Laundering Ecosystem: The Russian Case*, Center for Strategic & International Studies (CSIS), August 31, 2017, https://www.csis.org/analysis/exploring-information-laundering-ecosystem-russian-case.

[223] Jean-Yves Le Drian, closing speech of the international conference on “Civil societies, media, and public authorities: democracies facing the manipulation of information,” Paris, April 4, 2018.

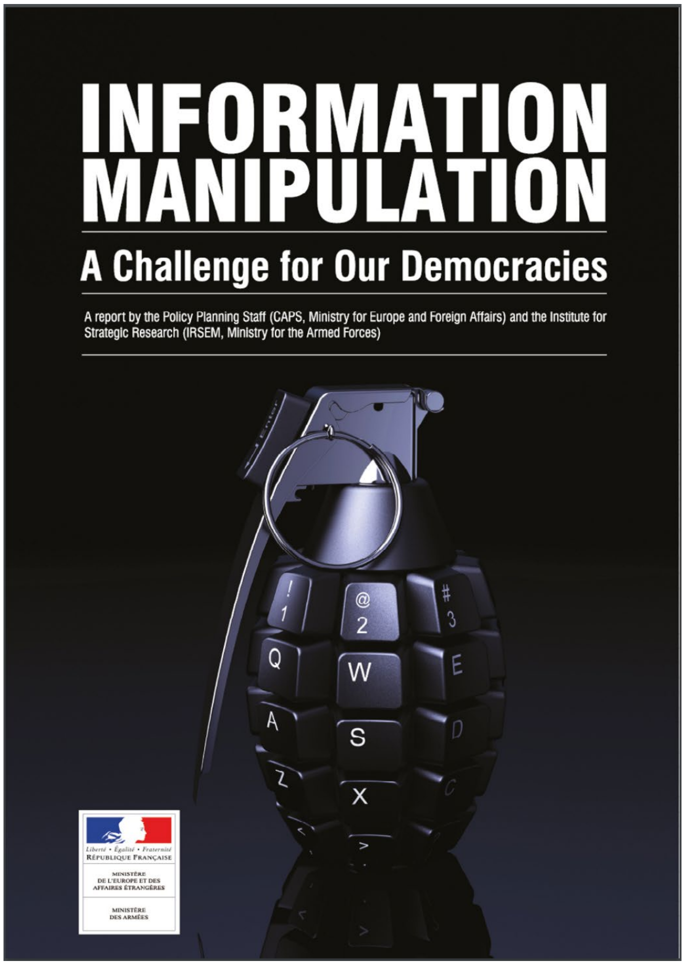
[224] Brattberg and Maurer, *Russian Election Interference*, 8.

[225] *Yellow vests flooded by fake news*, Avaaz report, 15 March 2019; “Disinformation export in 6 languages”, EUvsDisinfo, 17 April 2019.

[226] Tristan Berteloot, “’Pacte de Marrakech’, la trajectoire d’une fake news”, *Libération*, 14 February 2019.

[227] Annabelle Timsit, “The weirdest fake news controversies surrounding the new France-Germany treaty”, Quartz, 22 January 2019.

[228] “Building Blocks of Disinformation: Case of Notre Dame”, EUvsDisinfo.eu, 18 April 2019.



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

The main result is a 200-page report titled *Information Manipulation: A Challenge to our Democracies*, launched at the beginning of September 2018 and available online in French and English

> *“meddlers will not launch the same disinformation campaign twice: they will tailor their approach to each situation.”*

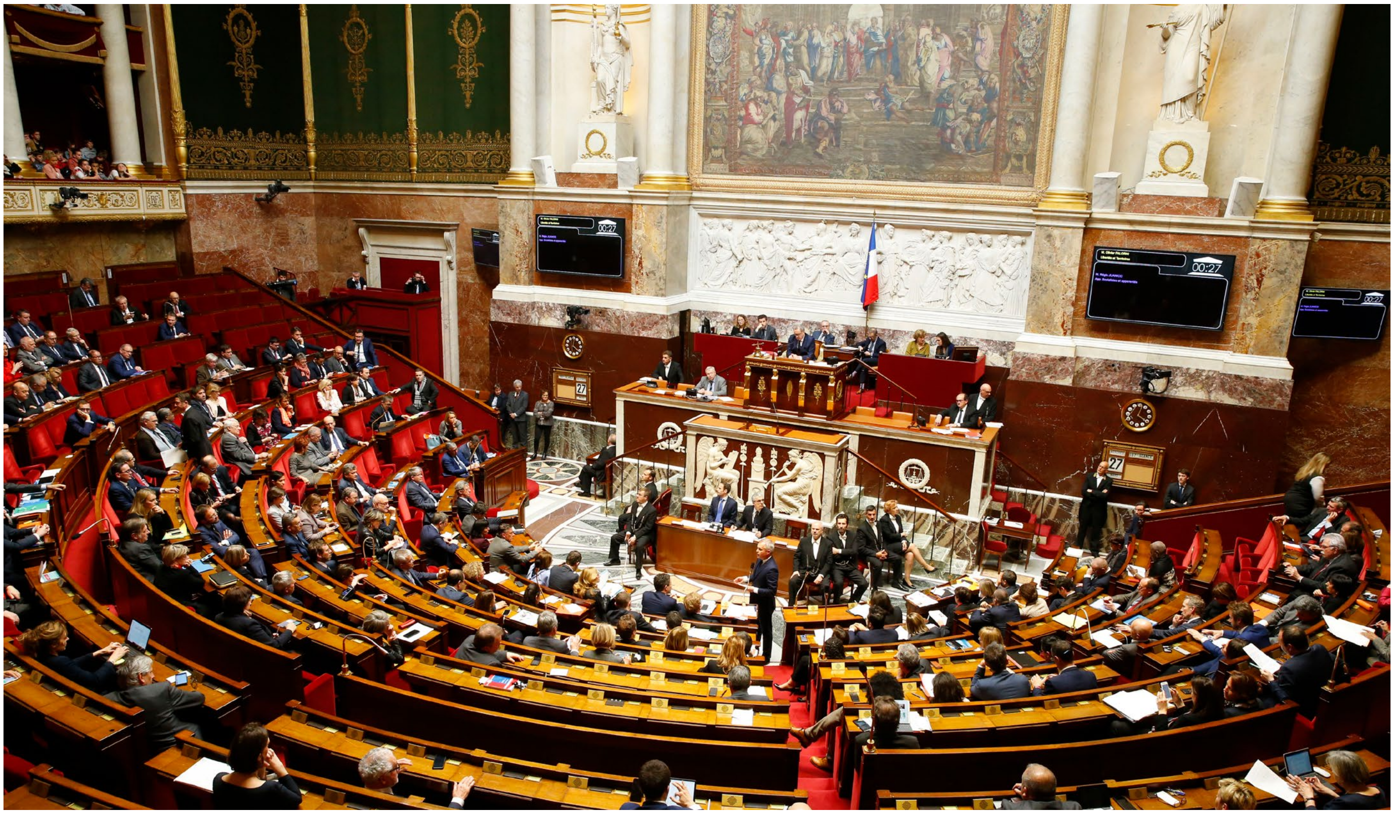
As a second caveat, it should never be forgotten that Macron was facing Le Pen, the far-right candidate, for whom most people are (still) not ready to vote. Macron consistently polled at twenty to twenty-five percentage points higher than she did[229] and he logically won by a huge margin. That is not at all comparable to the 2016 American presidential election, which was quite a close race, with the winner losing the popular vote. Even with weaker preparation and response from the French authorities, Macron’s campaign staff, and French civil society, especially journalists, Macron would likely have still won, if by a smaller margin. But the French political landscape can evolve, and complacency would be a mistake. Already, the National Front has changed its name and is attempting to enter the mainstream, with some successes in attracting “normal” right-wing politicians. In the same situation in the 2022 presidential election, with a more socially acceptable far right and a better candidate, the margin could be much smaller—and an influence operation like this one could be decisive.

The third caveat is that the threat will grow, for several reasons. France’s adversaries will learn from their mistakes. They will adapt, improve, and professionalize their techniques. They have already reduced the language gap by launching an RT TV channel in French, which—while careful of the scrutiny in what it publishes—is progressively growing a network of like-minded, French-speaking, pro-Russian individuals from across the political spectrum. The pattern of 2016-2017—massive leaks preceded by an RT/Sputnik propaganda campaign—will probably not repeat itself, as it has become too obvious. Instead, saboteurs are likely to act more discreetly, under cover of legitimate viral movements (such as #MeToo), targeting specific individuals or infiltrating mainstream media outlets that are not (or, at least, are less obviously) linked to the Kremlin. In other words, meddlers will not launch the same disinformation campaign twice: they will tailor their approach to each situation. Their process, their form, and their targets will change. Western states will need to better adapt to and anticipate these information environments and become more resilient in the long term. They must remain flexible and not depend on rigid models. The challenge is to supplement institutional anticipation with a degree of creativity.

Another preoccupation is that because of technological developments and the rise of artificial intelligence, manipulations will become more sophisticated. Improvements in voice and video editing will make detecting misinformation all but impossible, eroding public trust.

Aware of these challenges, France is preparing itself. The remaining pages will explore several steps taken in recent months.

[229] Aleksandra Wisniewska *et al.*, “French presidential poll tracker 2017,” *Financial Times*, May 7, 2017, https://ig.ft.com/sites/france-election/polls/.



The proposed bill stirred controversy and was rejected twice by the Senate before being passed by the National Assembly on November 20, 2018. *Source: Reuters Marketplace - Panoramic*

1. FRAMING THE DEBATE: THE CAPS-IRSEM REPORT

In September 2017, the Foreign Ministry’s Policy Planning Staff (*Centre d’analyse, de prévision et de stratégie*, CAPS) and the Defense Ministry’s Institute for Strategic Research (*Institut de recherche stratégique de l’Ecole militaire*, or IRSEM, of which I am the director), launched a joint working group. This work was not commissioned by the government, contrary to a rumor later spread by certain outlets—and even the Russian government itself[230]—in the hope of discrediting our efforts. Rather, we acted on our own initiative. The idea was born in the summer of 2017. I had just published an article in the *Revue Défense Nationale*[231] and the CAPS was studying the issue from the perspective of civil society. We were convinced of the importance of the subject and our approaches were complementary. Therefore, we decided to work together, which was formalized in a joint internal memo, dated September 1, 2017. This memo announced the launch of an investigation and the preparation of a report. This is how the administration and our ministers were informed of our work. They greeted it with interest and we kept them regularly informed of our progress in the following months. The report was expected, sometimes impatiently, but at no time did they ask us anything. To prepare the report, we visited twenty countries and conducted about one-hundred interviews with national authorities and civil societies. The main result is a 200-page report titled *Information Manipulation: A Challenge to our Democracies*, launched at the beginning of September 2018 and available online in French and English.[232]

This report rejects the phrase “fake news” for being both vague and itself manipulated by populist leaders, who call all news they dislike “fake.” It prefers the term “information manipulation,” for which we have been

[230] CAPS and IRSEM have been described by Russian Foreign Ministry spokeswoman Maria Zakharova as “state bodies, possibly sensing a demand or maybe fulfilling an order” (September 7, 2018, briefing, Moscow).

[231] Jean-Baptiste Jeangène Vilmer, “La lutte contre la désinformation russe: contrer la propagande sans faire de contre-propagande?” *Revue Défense Nationale*, No. 801, (June 2017), 93-105.

[232] Vilmer *et al*., *Information Manipulation* https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

advocating in our internal memoranda since the beginning of 2018. This term is more useful because most of the time the problem is not that the information is fake or false—just that it is exaggerated, biased, or sensationalized, tabloid-style. The manipulator does not care what is true and what is false; they are simply trying to produce an effect. It is no accident that in May 2018, a bill on this subject that was pending in parliament was renamed 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 report explores the causes and means of information manipulation, the responses, and future challenges. It concludes with fifty recommendations. There is a focus on Russia, not because we are “russophobic” but because in the interviews we conducted, as well as in the academic literature, Russia is considered the main threat. Most of the recent electoral interferences seem tied, directly or indirectly, to Russia.

The report identifies recurring vulnerabilities: disaffected national minorities (especially in the Baltic states); internal divisions (Poland’s political tensions, for example); external divisions (tensions between neighboring countries, unresolved historical issues, for example); vulnerable media ecosystems (tabloids in the United Kingdom, conspiracy websites in the United States); contested institutions (in Ukraine or the Baltic states, which provide fertile ground for the “failed state” narrative to take root).

Vulnerabilities are not enough. For manipulation to succeed, it requires the appropriate tools, of which Russia has many: government bodies; fake non-governmental organizations (NGOs); religious, political, or economic relays abroad; and so-called useful idiots. They can use white (overt), black (covert), or gray (in-between) propaganda. For gray and black propaganda anonymity is vital, particularly through fake media accounts.

Using these tools, Russia can create carefully calibrated narratives: anti-EU, anti-NATO, or anti-US; exaggerating immigration or crime; or exacerbating social and historical tensions. These narratives are often contradictory, and there are dozens of contradictory explanations of the Salisbury affair or the MH17 crash, for instance. Their priority is to be not consistent, but effective. One popular tactic is pitting communities against each other, supporting both sides of a social debate about, for example, race relations, LGBT rights, or refugees. The only objective is to divide and so weaken societies.

The CAPS/IRSEM report then considers responses. A general question is whether to respond or ignore the attack. Ignoring is a tempting option, given that refuting a story involves repeating and thereby sustaining it. “Strategic silence” may therefore be preferable in some cases. Yet this risks allowing such false and potentially dangerous ideas to sink into the minds of the population unchallenged. A strategy of ignoring should therefore be reserved for minor and inoffensive forms of information manipulation.

> *“The traditional compartmentalized approach is no match for adversaries using a full-spectrum or “hybrid” strategy, which blurs the line between war and peace.”*

A key part of the report looks ahead to future challenges. We distinguish technological challenges (deepfakes, artificial intelligence) from geopolitical challenges: the future trends in Russian information warfare. The latter can be grouped into four categories: (1) infrastructure—there is growing interest in the physical infrastructure of the internet, especially submarine cables and satellites; (2) personalization—sending text messages to Ukrainian soldiers to undermine their resilience and will to fight, or hiding personal attacks in legitimate movements such as #metoo; (3) going mainstream—the Kremlin is likely to go beyond RT and Sputnik and invest more in mainstream personalities, journalists, and media outlets to legitimize its narratives; and (4) using proxies—the use of other territories, most notably in Africa, where the population is less educated and therefore easier to influence, highly connected, and ripe with ethnic and religious tensions, as well as postcolonial resentment, all of which can be easily instrumentalized to hurt European values and interests.

The report ends with fifty recommendations, including twenty for states. These include:

- Avoiding heavy-handedness: Civil society (journalists, the media, online platforms, and NGOs) must remain the first line of defense against information manipulation in liberal, democratic societies. The most important recommendation for governments is to retain as light a footprint as possible—for the sake of their values but also out of a concern for effectiveness;

- Creating a dedicated structure, inside the government, to detect and counter information manipulation;
- Increasing transparency: making registration compulsory for foreign media, following the American example; conducting parliamentary inquiries; holding platforms accountable (for example, by demanding that they publicize the sources of their advertising and requiring them to contribute to media literacy and quality journalism);
- Going international: states must increase their participation in existing initiatives such as the EU East StratCom Task Force, the European Centre of Excellence for Countering Hybrid Threats in Helsinki, the NATO Strategic Communications Centre of Excellence in Riga. They should also send experts to compare notes and experience in important annual meetings in Prague, Riga, Washington, DC, and Singapore, to name a few; and
- Media literacy and critical thinking should be taught to adults as well as children; states could also support research (increase funding) on this issue, etc.

2. ACTING: LEGISLATION, MEDIA LITERACY, AND INTERNAL ORGANIZATION

In January 2018, the president announced his intention to pass legislation by the end of the year to tackle “fake news.” The proposed bill stirred controversy and was rejected twice by the Senate. A “Law against the manipulation of information” was finally approved by the National Assembly on 20 November 2018. One month later, the Constitutional Council confirmed its legality. Under this law, information manipulation is defined as the “inexact or misleading allegation of a fact that could alter the sincerity of an upcoming vote and that is spread deliberately, artificially or automatically and massively to the online public through a communication service.”[233]

In electoral periods, in the three months preceding the ballot, candidates and political parties can now appeal to a judge to stop “false information”; the CSA (the French Media Regulatory Authority) can suspend television channels “controlled by a foreign state or under the influence” of that state if they “deliberately disseminate false information likely to affect the sincerity of the ballot.” This is limited, however, to false news that are (i) manifest, (ii) disseminated deliberately on a massive scale, and (iii) leading to a disturbance of the peace or compromising the outcome of an election—three cumulative conditions that may be so difficult to satisfy in practice that the widespread accusations that such a law will threaten the freedom of the press are ridiculous, and the mechanism may prove to be rather inefficient. Any offense is punishable by one year’s imprisonment and a fine of €75,000.

Moreover, the law requires digital platforms to provide users with “information that is fair, clear and transparent” on how their personal data is being used, and to report any sponsored content by publishing the name of the author and the amount paid. A distinct decree, that came into force on April 15, 2019,[234] specifies that this is applicable to platforms exceeding the threshold of five millions of unique visitors per month in France, and that transparency obligations start for amounts of remuneration over €100 before tax.

Another significant initiative concerns media literacy. In March 2018, the culture minister pledged to double her ministry’s budget for media and information literacy, from €3 million to €6 million.[235] These funds will be used to support civil society actors (i.e. associations and journalists) working with schools and libraries to create a “civic service program” with the aim of mobilizing at least four-hundred young people to work on media literacy with libraries and media professionals throughout the country. It will also support public broadcasting companies in their educational role. Another part of the “media literacy plan” was the launch in June of a dedicated platform on the Franceinfo website. France is catching up, but much more needs to be done, as media education is still not part of the curriculum in too many French schools.[236]

Last but not least, the government also started to change its internal organization, making it less

[233] For a detailed analysis of the French law, see Marine Guillaume, *Combating the manipulation of information - a French case*, Strategic Analysis 2/2019, Hybrid CoE, Helsinki, 3 May 2019.

[234] Décret n° 2019-297 du 10 avril 2019 relatif aux obligations d’information des opérateurs de plateforme en ligne assurant la promotion de contenus d’information se rattachant à un débat d’intérêt général, *Journal officiel*, 11 April, 2019.

[235] Françoise Nyssen (minister of culture), speech at the “Assises du journalism,” Tours, March 15, 2018.

[236] Delphine Bancaud, “Pourquoi l’éducation aux médias est-elle toujours à la traîne en France?” *20minutes.fr*, February 21, 2019.

compartmentalized. As the CAPS/IRSEM report notes, there is an international consensus on the need for a more coordinated approach. France, too, is beginning to understand that it needs to adapt and to change its bureaucratic culture to fight against information manipulation. The traditional compartmentalized approach is no match for adversaries using a full-spectrum or "hybrid" strategy, which blurs the line between war and peace. To adapt to this fluid threat, agencies should cooperate and use new and unconventional methods that break down the traditional departmental divisions.

3. INTERNATIONALIZING: A CONCRETE PROPOSAL

The CAPS/IRSEM report recommended that states internationalize more, not only to learn from each other but also because we're stronger together, in particular to obtain more cooperation from giants like Facebook or Twitter. In line with this, I would like to suggest that France and some of its like-minded allies from both sides of the Atlantic could further progress in the fight against information manipulation by launching a joint initiative.[237]

First, a joint declaration or op-ed by the heads of state or government would announce a common agenda to fight information manipulation, and more generally the digital threats against our democracies. It would recall the existing initiatives in larger formats, such as NATO, EU, and G7, while highlighting the need for a fresh impetus.

It would then list the common measures that these states recently took and/or are about to take. There are country-specific differences of course but are enough similarities to identify the common denominators and present a united front. These measures are about cybersecurity, preventing electoral interference, digital platforms (suppression of illegal content, ads transparency, detection and labelling of bots), media literacy (common programs), research (common funding), etc.

These states would then commit to have regular meetings to share threat perceptions and good practices, some of them in track 1.5 format, with a mix of officials and civil society analysts, to infuse out-of-the-box ideas.

[237] Ben Scott (former coordinator of the Tech & Innovation Policy Advisory Group for Hillary Clinton during the 2016 presidential campaign) and I had this idea at the Canadian cabinet retreat in Nanaimo, BC, on 21-23 August 2018, where we were both invited to present the French and American experiences to the Canadian government. It was initially conceived as a French-Canadian initiative.

About the Author

Dr. Jean-Baptiste Jeangène Vilmer is director of the Institute for Strategic Research (IRSEM) at the French Ministry of the Armed Forces, and a nonresident senior fellow at the Atlantic Council. Trained in philosophy (bachelor, master, PhD), law (bachelor, LLM, post-doctorate), and political science (PhD), he served as policy officer on security and global affairs at the Policy Planning Staff (CAPS) of the French Ministry of Foreign Affairs (2013-2016) and has held positions at the faculty of law at McGill University, Canada (2011-2013), the department of war studies of King’s College, London (2010-2011), the MacMillan Center for International and Area Studies at Yale University (2008-2009), the French Embassy in Turkmenistan (2007-2008), and the University of Montreal (2005-2007). A member of the academic advisory board of the NATO Defense College and a lecturer at Sciences Po and the Ecole normale supérieure, Vilmer has authored some one hundred articles and nineteen books, and has received several awards (including the “Maréchal Foch” prize from the Académie française in 2013, and a nomination as a Munich Young Leader at the 2018 Munich Security Conference). He was the lead author of the French interministerial CAPS-IRSEM report, *Information Manipulation: A Challenge for Our Democracies* (2018).

IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE
DE L’ÉCOLE MILITAIRE

The Institute for Strategic Research (Institut de recherche stratégique de l’École militaire), known as IRSEM, is the research institute of the French Ministry of the Armed Forces. Composed of forty five 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, contributes to higher military education and engages in public debate on questions related to defense and security.

Atlantic Council Board of Directors

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org