CSIS BRIEFS

Successfully Countering Russian Electoral Interference

15 Lessons Learned from the Macron Leaks

By Jean-Baptiste Jeangène Vilmer
With an introduction by Heather A. Conley

JUNE 2018

THE ISSUE

The 2017 French presidential election remains the clearest failed attempt by a foreign entity to influence an electoral process in recent years. Taking aim at presidential candidate Emmanuel Macron, Russian interference succeeded neither in interfering with the election nor in antagonizing French society. This Brief examines how France successfully withstood the disinformation and interference; how this failed attempt can be explained; and, looking to the future, what lessons can be learned from this experience?

INTRODUCTION

On Friday, May 5, 2017—just two days before the second and final round of the French presidential elections—gigabytes of data hacked from Emmanuel Macron's presidential campaign team were released online. Months earlier an orchestrated disinformation campaign against the Macron presidential campaign had already begun. The so-called Macron Leaks—a combination of real emails and forgeries—could have been yet another example of a long list of attempts by Russia to interfere in a high-stakes transatlantic election. But the 2017 French presidential election may be the exception that proves the rule: it is the most clearly *failed* attempt. The Kremlin neither succeeded in interfering with the presidential election nor in dividing French society.

As the United States prepares to hold nationwide elections on November 6, 2018, the director of national intelligence, Dan Coats, has already warned in February of this year that "We expect Russia to continue using propaganda, social media, false-flag personas, sympathetic spokespeople and other means of influence to try to exacerbate social and political fissures in the United States." Calling Russian influence "pervasive," Director Coats further noted that "The Russians have a strategy that goes well beyond what is happening in the United States," he said. "While they have historically tried to do these types of things, clearly in 2016 they upped their game. They took advantage, a sophisticated advantage of social media. They are doing that not only in the United States but . . . throughout Europe and perhaps elsewhere." Because the United States is not well prepared for future elections, it is necessary to study the past.

This is why the 2017 French presidential election is a particularly important election to study and why we highlight French scholar Jean-Baptiste Jeangène Vilmer's groundbreaking report on the Macron Leaks.[1] Drawing in part upon the work of CSIS visiting fellow Boris Toucas,[2] Vilmer's forthcoming report will examine what happened during the French presidential election; who orchestrated the affair; how it was successfully countered; and what lessons can be learned. This Brief, which is part of the forthcoming CSIS comprehensive report, sums up the main lessons learned.

Myriad structural factors, luck, as well as effective anticipation and reaction by the Macron campaign staff, government and civil society, and especially the mainstream media, combined to successfully resist Russian malign influence.

-Heather A. Conley, CSIS

STRUCTURAL FACTORS

Compared to the United States or United Kingdom, France presents a less vulnerable political and media environment for a number of structural reasons. Unlike in the United States, the election of the French president is direct (e.g., there is no electoral college): attempts at interference or influence are more obvious, as they involve targeting candidates rather than constituencies. But most importantly, the French election has two rounds, which creates an additional difficulty for a malign actor to determine which two candidates will make it to the second round. The second round of voting also permits the population to dramatically shift their support to another candidate to block an unexpected result after the first round. The French media environment consists mainly of mainstream and critical media sources and is largely free of tabloid-style outlets and "alternative" websites that are common in the United States and United Kingdom. Culturally, critical thinking and a healthy skepticism are also deeply ingrained into French society at an early stage and throughout one's professional life.

LUCK

The Macron team was fortunate that those who hacked into their emails were sloppy and made a number of mistakes. Clearly, these individuals were overconfident and overestimated their ability to attract public attention and mobilize online communities. They also underestimated the resistance by French media and did not anticipate the Macron campaign staff reaction. Perhaps because the leaks revealed so little, there was an assumption that creating confusion would be sufficient. But the thousands of emails and other data appeared to have overwhelmed the public, enhancing their disinterest.

Releasing Macron's staff emails just hours before the electoral silence period was a risk. While the hackers did not want Macron to be able to defend himself, the limited time was also insufficient to spread the information. Moreover, the timing also rendered the entire revelation highly suspicious, the disinformation suffered from cultural clumsiness, and some of the fake documents were so absurd that the whole episode seemed amateurish. Interestingly, the accounts and bots that spread the misinformation were mostly in English because the leaks were first spread by the American alt-right community. Not only is this a completely ineffective means to reach a French-speaking audience, it also likely alienated French nationalist voters who are not inclined

The Macron team was fortunate that those who hacked into their emails were sloppy and made a number of mistakes.

to support anything American. France was lucky in the sense that this disinformation attack seemed hastily and clumsily formed. A more interesting question would be why was this organized so poorly? A last-minute decision due to the second-round vote? Other Russian agencies attempting to engage in similarly successful tactics but without the skills to pull it off?

Good fortune or not, France successfully anticipated, reacted, and coordinated its response between the Macron campaign staff, the government, and civil society. These are the lessons we learned from this experience:

ANTICIPATION

Lesson 1: Learn from Others. France had an advantage in that it was targeted after cyberattacks and disinformation campaigns were launched in the Netherlands, the United Kingdom, and the United States. All these precedents raised government and public awareness, but the 2016 U.S. presidential campaign was a game-changer. Prior to the U.S. election, awareness of Russian disinformation and malign influence was mostly limited to the Baltic and Central European states. Since then, large Western European states have learned that they too are vulnerable to disinformation. Paris benefited from the errors made by the United States: an overconfidence that disinformation campaigns would not work in the United States; reluctance to address the hacking of the Democratic National Committee; and a very delayed and muted response by the government.

Lesson 2: Use Trusted and Independent Administrative Actors. The Obama administration did not intervene in the U.S. electoral process even when the process was under siege because it did not wish to give the impression of advantaging the Democratic candidate. However, the French precedent shows that a state can intervene and take measures effectively provided that these measures are carried out by *administrative, independent, and nonpolitical authorities*. In France, these authorities provided technical and politically neutral expertise to ensure the integrity of the electoral process from start to finish. Two bodies played a particularly crucial role in France: the National Commission for the

Control of the Electoral Campaign for the Presidential Election (CNCCEP), a special body set up in the months preceding every French presidential election to serve as a campaign watchdog; and the National Cybersecurity Agency (ANSSI), whose mission is to ensure the integrity of electoral results and to maintain public confidence in the electoral process.

Paris benefited from the errors made by the United States.

Lesson 3: Raise Awareness. ANSSI and CNCCEP frequently alerted the media, political parties, and the public to the risk of cyberattacks and disinformation during the presidential campaign. ANSSI was particularly proactive, offering to meet with and educate all campaign staffs at very early stages of the election. In October 2016, ANSSI organized an open workshop on cybersecurity. All but one party participated (Marine Le Pen's *Front National* party rejected the offer). During the campaign, in early February 2017, ANSSI paid a visit to the Macron campaign headquarters to warn them about a potential attack. They were told that they were being watched, there was a risk of being hacked, and to be particularly careful using the Telegram app, which is Russian designed.[3] After this briefing, the Macron team switched from Telegram to WhatsApp, an end-to-end encrypted service owned by Facebook.[4]

Lesson 4: Show Resolve and Determination. From the start of the presidential campaign, the French government signaled—both publicly and through confidential diplomatic channels—its determination to prevent, detect, and, if necessary, respond to foreign interference. In an important speech on cyber defense in December 2016, the minister of defense announced the creation of a cyber command composed of 2,600 "cyber fighters." A few weeks later, the minister publicly remarked 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 . . . through our cyber arsenal but also by conventional armed means."[5] One month later, when Macron's political movement *En Marche!* announced that it was the target of an orchestrated attack, the minister of foreign affairs told the French Parliament that "France will not tolerate any interference in its electoral process, no more from Russia than from any other state"[6] A similar message was conveyed privately by the minister to his Russian counterpart and by President Hollande to President Putin.

Lesson 5: Take (Technical) Precautions. ANSSI heightened security at every step of the electoral process in order to ensure the integrity of the vote. The head of ANSSI stated before Parliament that he was "personally" opposed to voting machines and electronic voting.[7] Despite the unpopularity of the measure, the Ministry of Foreign Affairs followed his recommendation and, by March 2017, the government announced the end of electronic voting for citizens abroad because of the high risk of cyberattacks.

Lesson 6: Put Pressure on Digital Platforms. Ten days before the vote, Facebook announced that it "[had taken] action against over 30,000 fake accounts" in France. It was later revealed that the actual number of suspended French Facebook accounts was actually 70,000.[8] Facebook had never taken such a drastic measure before but it responded to growing pressure by both states and the public to take decisive steps as digital platforms are the principal medium for the spread of disinformation.

Polling station during the second round of the French presidential election.

Source: Jean-Francois Monier/AFP/Getty Images

REACTION

Lesson 7: Transparency and Timeliness Are Essential: Make All Hacking Attempts Public. Throughout the campaign, the *En Marche!* team communicated openly and extensively about its susceptibility to hacking and, soon after, about the hacking itself. They made public all hacking attempts against them, which generated awareness among the population and the authorities. When the Macron Leaks occurred, the *En Marche!* campaign reacted in a matter of hours. At 11:56 pm on Friday, May 5, only hours after the documents were released online and 4 minutes before the electoral silence—the French legally mandated period of 48 hours of reflection prior to an election where the media and campaigns are silent—went into effect, the Macron campaign issued a press release stating that "The movement has been the victim of a massive and coordinated hacking operation."[9]

Lesson 8: Beat Hackers at Their Own Game. The Macron Leaks were a combination of real emails and forgeries. But many of fake emails were so obviously fake—for example, the e-mails confessed to detailed accounts of untoward sexual practices or buying cocaine—that they actually helped the Macron team. Real emails in the hacked cache that could have damaged the Macron campaign, such as one that argued that "it is necessary that we lay off as many employees as we can after May 5,"[10] could not immediately be assumed authentic, so the controversy did not take root. In a risky move, the campaign staff went a step further. Knowing that they would be hacked, the campaign forged emails and fake documents themselves to confuse the hackers with irrelevant and even deliberately ludicrous information. By placing false flags, the campaign wished to inundate, confuse, and impede the work of the hackers with false information and slow them down. The campaign's strategy of "counter-retaliation for phishing attempts"[11] is known as cyber or digital blurring. It worked by turning the burden-of-proof tables on the hackers. The Macron campaign staff did not have to explain potentially compromising information contained in the Macron Leaks; rather, the hackers had to justify why they stole and leaked information that seemed, at best, useless and, at worst, false or misleading. The whole thing made the population doubt the authenticity of any of the leaked material.

Lesson 9: Strike Back on Social Media. The forceful presence of the Macron campaign staff on social media enabled them to respond quickly to the spread of disinformation. They tried to respond to as many posts or comments as possible that mentioned the "Macron Leaks," so as not allow trolls to have the last word.

Lesson 10: Use Humor When Possible: Readership Improves. In certain instances, the Macron campaign's injection of humor and irony into their responses increased the visibility and popularity of those responses across different platforms with undertones of mocking the amateurish attempts to influence the election.

Lesson 11: Law Enforcement Must Engage Immediately. Within a few hours of the initial email release, the public prosecutor's office in Paris opened an investigation, which was entrusted to the Information Technology Fraud Investigation Brigade of the Paris Police.

Lesson 12: Undermine Propaganda Outlets. On April 27, RT and Sputnik were denied accreditation by the Macron team to cover the remainder (until May 7) of its 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."[12] Even after the election, both outlets have been occasionally banned from the Élysée's Presidential Palace and Foreign Ministry press conferences.

This has been a controversial decision that fueled the Kremlin's narrative that France is doing exactly what it criticizes Russia for doing, allowing Russian President Putin an opportunity to lecture France on freedom of the press. However, the decision to ban RT and Sputnik from covering certain events was justified on the basis that these are propaganda entities and not media outlets as President Macron publicly stated following his meeting with Putin at Versailles only weeks after his election. This is also the position the European Parliament adopted as early as November 2016.[13] Moreover, attendance at these press conferences is by invitation only so there is no requirement that all outlets participate and RT and Sputnik are still permitted to operate in France.

Lesson 13: Trivialize the Leaked Content. The *En Marche!* press release said that the leaked documents "reveal the normal operation of a presidential campaign." Nothing illegal, let alone interesting, was found among the documents. Fortunately for the Macron campaign (which was not necessarily true with U.S. election disclosures), the fact that nothing compromising was found in the emails improved Macron's positive image as an authentic and "clean" candidate, compared to earlier scandals involving another presidential candidate.

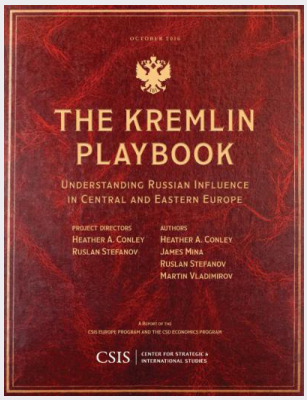
There was a disinformation campaign, data hacking, and large-scale leaking but there was no whitewashing or mainstreaming. The sequence was disrupted.

Lesson 14: Compartmentalize Communication. There was nothing scandalous in the leaked emails because Macron's campaign staff was aware from the beginning that it was likely to be vulnerable to hacking. Understanding that everything staff wrote could one day be hacked and leaked, the Macron campaign developed "three levels of communication: the trivial and logistical by email, the confidential on the [encrypted] apps, and the sensitive, only face-to-face."[14]

Lesson 15: Impress Upon the Media the Liabilities of Irresponsible Behavior. The night of the release of the emails, Macron's team referred the case to the CNCCEP, which issued a press release the following day, asking "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." The majority of traditional media sources complied, and some even drew their readers' attention to the timing of the leaks, asking them to exercise caution before responding to what might be a disinformation and destabilization operation directed against the French democratic process.

CONCLUSION

Using the 2016 U.S. presidential election as "a reference case," Finnish researcher Mika Aaltola has identified five 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; and (5) secret colluding [between a candidate and a foreign state] in order to synchronize election efforts."[15] According to this scale, the Macron Leaks reached stage three: there was a disinformation campaign, data hacking, and large-scale leaking but there was no whitewashing or mainstreaming. The sequence was disrupted between stages three and four. What was successfully prevented was "information laundering," the process by which the initial traces of foreign disruption are "washed" from the information, stories, and narrative.[16] This was prevented due to the aforementioned countermeasures and the resilience of the French media environment. ■



LEARN MORE

THE KREMLIN PLAYBOOK

Understanding Russian Influence in Central and Eastern Europe

The United States can no longer be indifferent to these negative developments, as all members of NATO and the European Union must collectively recognize that Russian influence is not just a domestic governance challenge but a national security threat. To learn more about Russian influence in Central and Eastern Europe, please review CSIS's flagship report, *The Kremlin Playbook*.

Jean-Baptiste Jeangène Vilmer *is the director of the Institute for Strategic Research (IRSEM) at the French Ministry of Defense. The views expressed in this Brief are the author's own and do not represent those of any institution to which he is or was affiliated.* ***Heather A. Conley*** *is senior vice president for Europe, Eurasia, and the Arctic and director of the Europe Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.*

ENDNOTES

1. Jean-Baptiste Jeangene Vilmer, "The Macron Leaks: A Post-Mortem Analysis," CSIS Europe Program, forthcoming.

2. Boris Toucas, "The Macron Leaks: The Defeat of Informational Warfare," *CSIS Commentary*, May 30, 2017, https://www.csis.org/analysis/macron-leaks-defeat-informational-warfare.

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

4. Ibid.

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

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

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

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

9. En Marche!, "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.

10. Raulin and Gendron, "Piratage."

11. Mounir 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.

12. Macron spokesman in Andrew Osborn and Richard Balmforth, "Macron camp bars Russian news outlets, angers Moscow," Reuters, April 27, 2017.

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

14. Raulin and Gendron, "Piratage."

15. Mika Aaltola, *Democracy's Eleventh Hour: Safeguarding Democratic Elections against Cyber-Enabled Autocratic Meddling*, Briefing Paper 226 (Helsinki: Finnish Institute of International Affairs, November 2017), https://storage.googleapis.com/upi-live/2017/11/bp226_democracys_eleventh_hour.pdf.

16. Boris Toucas, "Exploring the Information-Laundering Ecosystem: The Russian Case," *CSIS Commentary*, August 31, 2017, https://www.csis.org/analysis/exploring-information-laundering-ecosystem-russian-case.