Global Challenges
Election Disinformation

INNOVATIONS FOR
SUCCESSFUL SOCIETIES

DEFENDING THE VOTE: FRANCE ACTS TO COMBAT FOREIGN DISINFORMATION, 2021 – 2022

Alexis Bernigaud drafted this case study based on interviews conducted in France from August through November 2022. Case published January 2023.

SYNOPSIS

After a hack-and-leak operation that targeted a candidate in its 2017 presidential election and a social media campaign against its exports in 2020, France's government decided to take steps to protect its politics from foreign digital interference. With another national election approaching in April 2022, Lieutenant Colonel Marc-Antoine Brillant began designing a new unit that aimed to detect foreign information manipulation while preserving freedom of speech by separating responsibility for identification of attacks from responsibility for framing and executing a response. After the proposal cleared legal hurdles, Brillant's team, under the authority of the Secretariat-General for National Defense and Security, set up an interagency governance system, initiated a dialogue with social media platforms, and monitored social media to detect hostile campaigns. During the 2022 campaign, the unit, called Viginum, identified five foreign interference attempts and referred them to other parts of government that could decide whether and how to react. The elections ran smoothly, and the Viginum team started to focus on building stronger public understanding of its mission and activities.

ISS is program of the Princeton School of Public and International Affairs: successfulsocieties.princeton.edu. ISS invites readers to share feedback and information on how these cases are being used: iss@princeton.edu.

INTRODUCTION

On Friday, May 5, 2017, just two days before the second and final round of the French presidential election, an anonymous user released on file-sharing website Pastebin.com 15 gigabytes of data and 21,075 emails stolen from Emmanuel Macron's campaign staff. The news quickly spread on Facebook and Twitter with hashtag *#MacronLeaks*. The emails were made public only hours before a legally mandated, 44-hour preelection media blackout. France's campaign watchdog, the National Commission for Control of the Electoral Campaign, set up in advance of each presidential election, issued a statement reminding media outlets and citizens of their responsibility to protect the vote against the dissemination of potentially false information.[1] In the end, the *#MacronLeaks* operation did not significantly affect the outcome of the election, which Macron won with 66.1% of the votes. Although the operation was never formally attributed to Russia, many analysts said the Kremlin or the American alt-right were most likely behind it.[2]

Three years later, on October 16, 2020, Samuel Paty, a teacher who had shown cartoons depicting Muslim prophet Muhammad in class was murdered by a terrorist in the French town of Conflans-Sainte-Honorine. On October 21, Macron gave a speech in which he reaffirmed France's refusal to condemn such cartoons. His stance drew immediate criticism from several countries in the Muslim world, including Egypt, Libya, and Yemen.[3] The president of Turkey was particularly vocal, publicly questioning Macron's mental health and encouraging the boycott of French products.[4] Hashtag *#boycottfranceproducts* became viral in several countries, and the French government suspected that foreign states were artificially amplifying the campaign.

After the attack, representatives of several French ministries alerted the Secretariat-General for National Defense and Security—an interministerial body under the authority of the prime minister—to the ubiquity of aggressive anti-French narratives on social media. Secretary-General Stéphane Bouillon recommended creating a task force to analyze the campaign and identify its source.

With the prime minister's approval, Bouillon quickly set up an interministerial crisis unit initially responsible for investigating the anti-French campaign. Called Honfleur, after the name of the room where it launched its mission, the task force had limited resources and little experience in the analysis of foreign information manipulation. Nonetheless, in just a few months, Honfleur, led by Lieutenant Colonel Marc-Antoine Brillant, managed to show the way that hostile narratives were being artificially amplified via internet bots and other devices. Honfleur also mapped the sources of specific types of content and identified the target audiences of the operations. (Text Box 1)

Based on the task force's findings, in January 2021 President Macron decided to launch a permanent unit within the Secretariat-General for National Defense and Security that could detect and monitor foreign online information manipulation. Bouillon assigned Brillant responsibility for proposing the design of the unit and for redefining the interministerial governance structure, with a view to protecting the country from foreign digital interference.

Text box 1: The Honfleur task force

In November 2020, Secretary-General for National Defense and Security Stéphane Bouillon named Marc-Antoine Brillant head of the Honfleur task force. The group initially had a clear and narrow mandate: to understand the anti-French campaign and its potential instigators and contribute to a response. The Ministries of the Interior, Armed Forces, and Foreign Affairs along with the government information service and the Secretariat-General for National Defense and Security provided staff to take part in the task force.

Both Lieutenant Colonel Marc-Antoine Brillant, who was serving as adviser for the Secretariat-General for National Defense and Security, and Claire Benoit, who was working on hybrid threats as a desk officer at the same secretariat, participated in the task force and later became part of Viginum.

The task force had two parallel missions. The first was to draw up an inventory of France's informational and technical capacities in order to identify institutional partners that could provide relevant information. The second was to create a methodology in the form of a set of protocols for identifying foreign disinformation campaigns. "We started with a blank slate," said Brillant. "We were like a forensics team working with things we could easily observe on social media—while trying to go beyond the mere content that was shared—in order to learn the mechanics behind its diffusion and, if possible, the origin of the campaign."

The team focused on four parameters:

- Content: Not the accuracy of the information shared but, rather, the intent behind it
- Origin: Pinpointed on a map of actors on specific platforms
- Propagation dynamic: The way the content was shared and amplified; identification of accounts with central roles in the diffusion of content or because they connected different audiences
- Target audience: The specific keywords used for bringing together unrelated audiences under the same campaign, as identified through semantic analysis tools

Using this methodology, the task force managed (1) to show how hashtag *#boycottfranceproducts* was spread using artificial means and (2) to connect it to a map of actors that showed that Türkiye played a central role in the campaign.

THE CHALLENGE

Online content regulation was a sensitive issue in France. Back in 2018, in response to the *MacronLeaks* operation, the government had introduced a bill on information manipulation, which gave additional powers to the media regulator called the Superior Audiovisual Council, later known as Arcom following a merger with France's internet copyright protection agency.[5]

The proposed law had four significant elements. First, it allowed Arcom to suspend the distribution of media outlets owned or controlled by foreign states in the three months leading to an election if the states spread false information that could affect the fairness of the election. Second, it required online platform operators to inform the public of the sources and targets of paid-for online content relevant to a forthcoming election. Third, it required online platform operators to report annually to the media regulator on progress in such areas as preventing the transmission of false information and promoting content from reliable sources. And fourth, it established a fast-track judicial procedure to take down false information during elections.[6]

The bill attracted intense criticism from opposition parties, and the French Senate rejected it twice because of doubts about "the effectiveness of the proposed provisions" and the "risks of disproportionate constraints on freedom of speech," a constitutional right in France.[7] Although the bill eventually won legislative approval in late 2018, the issue remained controversial in 2021. "It could have been tempting for certain members of the public to say, 'As if by chance, the executive is creating a government agency to fight information manipulation less than a year before the election' and to compare it to a 'ministry of truth' or an office of censorship aiming to get the current president reelected," said Brillant.

Brillant and his team said they were aware of the threat of a political backlash and knew they had to build both public support and political backing. They also knew that the prime minister would have to issue a decree to formalize the unit's mission and that such a decree would have to balance the unit's goals with the need to protect free speech.

Fighting against information manipulation required efficient interministerial cooperation, which posed a second challenge for the design mission. A variety of public institutions—the Ministry of the Interior, Ministry of Foreign Affairs, Ministry of Armed Forces, and Arcom—had their own institutional mandates to deal with specific aspects of the threat.[8]

During the spring of 2018, the government created the Committee for Fighting Information Manipulation, which brought together representatives from the ministries of Culture, Education, Armed Forces, Interior, Justice, and Foreign Affairs as well as the government's information service. The Secretariat-General for National Defense and Security led the committee, with the goals of building a shared understanding of the threat and combining their monitoring efforts. The committee discussed policy responses, but its mandate never shifted to operational work. "The idea of putting more resources into the detection of information manipulation was raised, but because each service had its own prerogatives, none of them could cover the whole scope of the problem," said Claire Benoit, who provided secretariat support to the committee from September 2019 to 2020. The participants also discussed creating a dedicated unit or agency empowered to monitor disinformation, but they feared that such a unit would be perceived as a threat to freedom of speech. "Politically, we could not rush things without taking the risk of affecting freedom of speech. It was a sensitive issue," said Benoit.

An important aspect of the design work involved defining protocols for the new unit. Members of the Honfleur task force had not reviewed scientific evidence or international best practices to develop their ad hoc methodology. Defining how the new unit would identify and characterize foreign information manipulation was a major challenge for Brillant and his team.

Finally, although the project benefited from a high level of support from the executive, Brillant had to build a new unit from the ground up. His team had to determine the technical means required, negotiate a budget, hire staff, and find office space while keeping in mind that the unit had to become operational well before the April 2022 presidential elections.

FRAMING A RESPONSE

In early 2021, the Secretariat-General for National Defense and Security repurposed the Honfleur task force to start thinking about the design process for a new unit. "While the design mission officially started to work at the beginning of March, the task force transitioned into the design mission smoothly," said Benoit.

Building a team. Secretary-General Bouillon gave Brillant broad flexibility in building a team to design the new institution. "The excellent results achieved through the Honfleur task force helped us build…a trusting relationship," said Brillant, who aimed to get the new institution started by June or July 2021.

Brillant selected three individuals, each of whom brought distinctive skills and knowledge to the effort. Benoit, a member of the Honfleur task force, had been in charge of coordinating the Committee for Fighting Information Manipulation. In addition to her previous work on terrorism and hybrid threats, she had extensive knowledge of the interministerial aspects of the fight against information manipulation. David Robert, an engineer who had worked with the Ministry of the Interior and the Secretariat-General for National Defense and Security on information systems and digital transformation, focused on technical aspects of the preliminary mission. Brillant's third pick was Xavier Givelet, a senior manager from the prime minister's office and a former magistrate who had graduated from the École Nationale d'Administration (National School of Administration), France's school for high-ranking civil servants. Givelet had expertise in audit, public financial management, and administration, and he handled budgetary and logistical aspects of the design. In addition, the cabinet of the Secretary-General gave its full support to the team.

Exploring different models. The preliminary mission learned important lessons by evaluating other countries' efforts to address foreign online information manipulation. The UK had set up its National Security Communications Team in 2018 within the Cabinet Office, which supported the prime minister and his ministers.[9] The UK system was still in development but offered one model for securing interagency cooperation.

Spain's experience offered a cautionary tale about the need to involve members of parliament.[10] Controversy had erupted after Spain's National Security Council adopted an action plan against disinformation in November 2020. Opposition MPs argued that the government was creating a "ministry of truth" and attacking freedom of the press.

"This is what finally convinced the secretary-general that French MPs should be consulted—even before laying the first stone of the project," said Benoit. Working with legislators up front could help generate useful ideas as well as a sense of ownership.

The team looked at the United States, whose government was beginning to collaborate with universities, civil society groups, and social media companies such as Facebook and Twitter to identify and respond to disinformation. It also reviewed the work of the European External Action Service's East Stratcom task force, which analyzed disinformation trends and had exposed pro-Kremlin disinformation narratives since 2015, and it studied Singaporean, Swedish, and Taiwanese models.

Members of the design mission were especially interested in whether other countries were trying to fight foreign information manipulation, domestic disinformation, or both—as well as the protocols that governed their work. And although Macron's initial directive focused the new unit on foreign disinformation, it was still essential to develop clear criteria for distinguishing domestic from foreign disinformation and for focusing only on the latter.

Consulting with partners. Before Macron decided that the Secretariat-General for National Defense and Security would host the new unit, the government had considered other possible hosts. The matter was still causing some debate, and the secretariat-general took steps to ensure the new unit would maintain strong relationships with other ministries and agencies in support of their efforts to fight disinformation and not infringe on their individual mandates. "We had to go on the campaign trail," Brillant said.

The secretariat-general held a series of coordination meetings during the design phase and shared an initial draft of a decree creating the new unit, reaching out to relevant ministries ahead of an interservices meeting held in March 2021. During the March meeting, the Ministries of Armed Forces, Foreign Affairs, and the Interior shared their thoughts on the proposals. "We quickly reached an agreement on the main missions, which are to detect and characterize foreign information manipulation attempts, as well as on a major role for the unit during elections," he said.

The meeting participants achieved consensus on four elements.

1. The new unit would focus only on debates regarding the nation's fundamental interests, including the integrity of its territory, its security, and the republican form of its institutions as defined by article 410-1 of the French penal code.[11] That focus was intended to narrow the scope of the monitoring by

excluding most of the issues debated online such as politics, sports, and entertainment.

2. The new unit would work only on foreign threats and would refrain from monitoring information manipulation by domestic entities.

3. The new unit would use only open-source data that was publicly available and did not require interaction with other users, entry into private groups, creation of avatars, or management of human sources.

4. An interministerial Ethics and Scientific Committee, established within the Secretariat-General for National Defense and Security, would monitor the unit's work.

Building on his experience at France's cybersecurity agency, Brillant set up a new interministerial governance structure inspired by the Cyber Crisis Coordination Center, which fostered strategic and technical collaboration between government organizations.

At the same time, the team had to come up with a name for the new unit, a task that required careful deliberation. "We excluded such terms as *defense* and *fight* because we wanted to avoid a military connotation," Benoit said. "Because we knew the unit would protect the national online debate through vigilance, we named it the National Service in Charge of Vigilance and Protection against Foreign Digital Interference." Bouillon came up with a short version of the name, which was inspired by the secretariat-general's antiterrorist plan Vigipirate. "He took the words *vigilance* and *numérique* [*vigilance* and *digital*] to create Viginum, which is catchier than the full name," she said.

Consulting with political groups. Brillant joined Bouillon for a series of meetings with representatives from Parliament at which they explained the disinformation threat and described the key features of the planned service. "All political groups understood that the threat was serious, and they agreed that the creation of Viginum was necessary," Brillant said. The meetings helped pave the way for the passage of enabling legislation if such action became necessary later in the process.

Managing money and logistics. "In the French administration, you don't create a new unit every day," Givelet stressed. "We had to prepare a budget, to secure office space for the new unit—which had to be kept secret and meet strict security standards—and to plan for an efficient recruitment process—notably, through workforce simulation. We were like a state start-up: a very small team with very limited resources, working in meeting rooms with pens, paper, and a few laptops. We didn't even have an office at first. It was a first in my career."

The team had to negotiate the budget with the prime minister's office during a period of austerity caused by the COVID-19 pandemic. Brillant said, "We tried to ask only what we really needed, and we managed to secure a budget that was sufficient to get the unit started. We got what we needed to execute our mission."

Givelet emphasized the importance of cost control and smart spending. "I wanted to create an efficient administrative framework for the unit," he said.

"By putting automated systems in place, I wanted the unit to work well at minimum cost." Borrowing a procedure used in the information technology industry, he created a system of support tickets that team members could use for specific logistical needs, including office supplies, meeting rooms, or even problems related to heating. "By centralizing the requests, we wanted to make sure they would be dealt with efficiently," he said.

Translating the methodology into a decree. French law required a decree from the president or the prime minister to create a new government unit, define its prerogatives, and modify the secretary-general's mandate. With support from legal experts at the Secretariat-General for National Defense and Security and feedback from other ministries, the team drafted a decree[12] to create Viginum and define its responsibilities. The new unit's main mission would be to "detect and characterize, through the analysis of publicly available online content . . . campaigns involving a foreign entity to spread inexact or deceptive content" that could "harm the nation's fundamental interests" by using "artificial or automated systems." The draft decree also gave Viginum the responsibility to inform election authorities about foreign disinformation campaigns during electoral campaigns and to help coordinate interministerial work on protection against foreign disinformation campaigns.

To reassure citizens worried about issues involving free speech, the decree created an Ethics and Scientific Committee within the secretariat-general—as proposed in the early planning stage—to monitor Viginum's activities. The draft decree gave the committee the responsibility to make nonbinding recommendations regarding how Viginum carried out its missions and to draft an annual report to the prime minister that would be made public.

GETTING DOWN TO WORK

In July 2021, Macron issued decree number 2021-922, which officially created Viginum. When the secretariat-general started looking for suitable candidates to lead the permanent unit, Brillant was the logical choice, given his experience in leading both the Honfleur task force and the preliminary design mission. Shortly after the decree came out, Bouillon appointed Brillant deputy head of Viginum to oversee the initial organization and operation of the new agency. At the same time, Bouillon began recruiting a head for the unit. With the April 2022 presidential election in sight, he had no time to lose.

Gaining authority for automated data collection

To move the work forward, the team needed two authorizing decrees: one for creation of a new administrative entity and the second for creation of a legal framework for automated data collection. Because of stringent French laws protecting digital rights and other civil liberties, the second decree would likely involve a lengthy and complicated process and would take months of negotiation. Work on that decree began quickly.

The new draft decree had to authorize the collection of personal data on social media platforms. Members of the preliminary mission were already in contact with the secretariat-general's legal experts and the Commission on Informatics and Liberty—the independent administrative regulatory body that monitored compliance with data privacy laws.

Bouillon requested a formal—but nonbinding—opinion from the Commission on Informatics and Liberty. In October, the commission published its opinion,[13] which expressed a number of reservations and recommended full legislative review, notably arguing that the collection of data would have a "considerable impact on citizens' right to privacy and the protection of personal data," which "can be allowed only if it is strictly necessary to achieve the aim pursued and if sufficient guarantees are provided with regard to the safeguarding of the fundamental principles of data protection and privacy." The commission recommended "a democratic debate in Parliament" to "evaluate the proportionality of the measures and to set rules regulating and limiting their use, as well as to monitor procedures."

The Conseil d'État (Council of State), France's supreme court for administrative justice and legal adviser to the executive branch, also examined the draft. Its decision was particularly important because, among other things, it would determine whether a decree would be sufficient or whether the issue required parliamentary action. Given the amount of time required for passage of a law in Parliament and the need for Viginum to become operational before the 2022 presidential election, the team toiled to provide information on the unit's goals and needs for the commission and the Council of State.

After weeks of discussion, the council decided a decree would be sufficient.[14] In early December, the prime minister issued decree number 2021-1587,[15] which permitted Viginum to use automated data collection for identifying foreign digital interference.

To ensure that Viginum selected online content for analysis with minimal risk to political rights and civil liberties, the decree established a two-part process. For each issue investigated, Viginum's staff would first have to identify likely instances of disinformation by manually monitoring social media posts. For example, staff would check what people were saying on Twitter under hashtags related to a French election or an aspect of French policy. If they spotted posts that appeared to disseminate disinformation, they could look at the account that shared the content and assess whether this account had also posted content associated with a foreign government as well as whether there was evidence of automated amplification—such as whether the account shared the information around the clock and throughout each week. Based on elements gathered during the monitoring phase, Viginum could then decide whether the situation required automated data collection and determine the scope of the data collection exercise, establishing a list of technical criteria in the forms of account names, keywords, platforms, and time periods.

The decree placed several other limits on the use of automation. First, Viginum could use automated data collection only on platforms that had more than 5 million monthly individual users in France. It set time limits for such collection (seven days maximum, renewable up to six months) and banned the use of facial- and voice-recognition systems for selecting content. The decree also specified the categories of data that could be collected automatically such as personally identifiable information declared by the owners of accounts either sharing or reacting to publicly available content; data related to the audience; reach of accounts, including number of followers; and content shared by the accounts along with related audience indicators. The decree further required the deletion of data either after use or no more than four months after its collection. In addition, the decree required that Viginum inform the Ethics and Scientific Committee every time it began an automated data collection phase.

Redefining interministerial governance

In August 2021, as a result of the consultation process launched the previous March, the secretariat-general established a new interministerial governance model to fight foreign digital interference. The structure had three levels.

- On a technical level, the Monitoring, Detection, Characterization, and Proposal Network brought together Viginum and its counterparts in other ministries—including intelligence services—to share information on threats identified by different administrations as well as information on technical tools and methodologies.
- On an operational level, the Operational Committee for Fighting Information Manipulation, headed by the secretary-general for defense and national security, brought together the heads of services with operational capacities—notably, within the ministries of Armed Forces, Foreign Affairs, and the Interior. Based on Viginum's analytical reports and information or advice shared by the technical network, the operational committee assessed risks, discussed response strategies, and took concrete actions to neutralize the threats.
- On a political level, the preexisting Committee for Fighting Information Manipulation, created in 2018, convened a wider range of ministries and agencies, including the media regulator and the ministries of Education, Culture, and Justice. The committee focused on problems and policies related to societal resilience, including media literacy programs.

Creating a nimble organization

In early October, the prime minister appointed Gabriel Ferriol, a magistrate from the Court of Accounts—France's supreme audit institution—to head Viginum. Expanding the staff was a priority in order to prepare the organization for the approaching election. Since its creation, Viginum had focused on recruiting staff with diverse backgrounds: open-source investigators, digital marketers, data scientists, and IT specialists, as well as experts in political science and geopolitics. "It's difficult to recruit data scientists," Ferriol recalled. "We had to make ourselves known to attract talent." In addition to posting job openings on the official public-sector recruitment platform and LinkedIn, Viginum adopted an approach used by the private sector. It joined Welcome to the

Jungle,[16] a French website that helps companies attract new employees. On the site, Viginum recruiters shared pictures, videos, and details on the unit's work culture. The unit also launched staff-training programs that included courses on monitoring tools, open-source intelligence, cartography, and computer programming.

The unit grew from 8 employees in July 2021 to 23 by year-end, and the fast growth required special measures. "We staggered hires and welcomed successive waves of employees," said Ferriol. In September 2022, Viginum had 42 employees and was still working toward its target of 65.

Flexibility and speedy response were important goals of the organizers. "We made a choice that was pretty original," Ferriol said. "We could have divided our operational staff into several departments, each focusing on a single platform or a specific type of threat, but we wanted to have all of our agents in a single structure: the operations department."

The operations department, which comprised 74% of Viginum's staff, identified challenges and ways of dealing with them. "When we decide to analyze a campaign, we create what we call an *operation*," Ferriol said. Operations were time limited and focused on specific issues such as the online debate around social unrest in the French West Indies (December 2021–January 2022)[17] or the Paris terrorist attacks trial that took place from September 2021 to February 2022. During its first year, Viginum responded to some special situations, but its primary task was to protect the national election.

Managers designated supervisors for each project and assigned agents who had relevant expertise. "We could say, 'Now that we'll be working on this new subject, we're going to choose these four experts because they are familiar with the geopolitical context' or 'because they have investigation or language skills,'" Ferriol said. "In that case, we could create a team to focus on this threat for a few weeks or months."

Ferriol described the system as "extremely flexible. We don't have predefined teams, and we can react to the news, send backup to a team when it faces more pressure, or reassign staff members when they realize their operation doesn't lead to identification of a threat."

Two smaller groups supported the work of the operations department. A coordination and strategy department was in charge of interministerial and international cooperation. It also acted as a secretariat for the Ethics and Scientific Committee and managed Viginum's internal and external communications. A separate support department managed human resources, finances, and logistics.

Girding for the elections

Viginum's priority for the last quarter of 2021 was to become operational for the April 2022 presidential election. The unit reviewed international examples of election-related information manipulation and assembled a report on threats and the various strategies foreign adversaries use to destabilize elections. After identifying key concepts and processes, agents could test their responses in real-life situations. (Text box 2)

Text box 2: The Ethics and Scientific Committee

On July 13, 2021, the decree that created Viginum also created the Ethics and Scientific Committee within the Secretariat-General for National Defense and Security. Article 7 of the decree described the committee's composition, which reflected the interministerial nature of its mission. Members of the committee were appointed under a nonrenewable, five-year mandate.

The decree defined the committee's composition, which consisted of a president appointed by the vice president of the Council of State among councillors of state; a member of the media regulator appointed by its head; and six individuals "with expertise on Viginum's area of competence," appointed by the prime minister. The six with expertise consisted of two proposed by the Minister of Culture and one each by the ministers of foreign affairs; justice; higher education, research, and innovation; and the secretary of state for digital affairs.

The committee, which had access to all documents produced by Viginum, was informed when an operation was launched or closed, and it received information regarding automated data collection phases. It also received Viginum's reports and could formulate recommendations on Viginum's activity. The committee drafted an annual report that was sent to the prime minister and made publicly available.

"We didn't know what to expect from the committee at first, but everything went well," said Viginum head Gabriel Ferriol. "When the committee asks us questions, we answer and provide additional elements to explain our decisions. It's good to have an outside look when you are doing something new."

When the committee received reports or questions from Viginum, it discussed issues internally via email and organized meetings with all members to formulate recommendations for interpretation of the four criteria needed to characterize foreign digital interference or other aspects of the unit's work. "So far, Viginum has followed all of our recommendations," said committee head Béatrice Bourgeois-Machureau.

In November 2022, the committee was working on its first annual report. "Our report will include the content of the recommendations we presented throughout the year as well as Viginum's response. It will also reflect on the current legislation and suggest changes. One of the recommendations we will include in the report relates to the role of the committee. The second decree gave the committee the responsibility to monitor Viginum's data collection process, which implies analyzing technical documents almost daily. It is difficult for the committee to deal with this additional workload while focusing on its core missions. An expert working on this specific issue on a full-time basis could be a solution, or it could be in the form of a dedicated structure."

In September, Viginum worked with authorities from Germany and the European External Action Service—the European Union's diplomatic service—to help secure the September 26 German federal election. The unit analyzed French-language content on social media to see whether foreign entities were trying to use the French public debate to affect the German election. The collaboration generated insights into how the Germans operated and into the effectiveness of methodologies and tools, according to Benoit. Staff members also drew insights about the perpetrators of information manipulation, their modi operandi, and the methods used in detecting inauthentic behaviors.

"The real dress rehearsal for Viginum happened in December 2021, when we worked on New Caledonia's referendum on independence from France," Ferriol said. Putting theory into practice enabled Ferriol's team to clarify distinctions between the detection and characterization phases of their work and to standardize the types of documents used in the process. Ferriol said the exercise helped get everyone on the same track. "Our new recruits were coming from extremely diverse backgrounds, where the terms *detecting* and *characterizing* had different meanings. We were all speaking slightly different languages," he said.

The operation also enabled the team to gain valuable experience and to experiment with new methods. "We started to organize shifts so as to have staff on-site during weekends," Ferriol said. Given the time difference between France and New Caledonia, half a world away, the team had to work at night during the referendum.

"To organize night and weekend shifts, we had to install beds, provide food for our agents, and set up specific security procedures," said Givelet. "It was like a test for us, and we learned a lot from this first experience." And in an election that proceeded peacefully despite initial fears of violence, voters in New Caledonia rejected independence.[18]

After those experiments, the unit formalized the two main phases of its work: detection and characterization. Getting both of them right was crucial to Viginum's success.

During the detection phase, staff members browsed the web and identified situations that were atypical in the context of the online public debate. Accounts attracted suspicion if they appeared to have been forged or created through an automated process because their accompanying profile picture had been generated by artificial intelligence or because their behavior was unusual. "A typical example of aberrant behavior is an account that is posting content 24/7 without sleeping," said Ferriol. By identifying accounts that systematically mirrored the behavior of other accounts, Viginum staff could infer that users of the accounts were coordinating their efforts to distort the online debate. Content that appeared to be manifestly false also drew the attention of agents.

Based on what they found through manual monitoring and with supervisor approval, staff members could target specific accounts or topics and use automatic data collection to gather additional evidence. Selectivity was crucial to the process. "We want to avoid ending up with a disproportionate heap of data," said Brillant. "We save time by extracting seemingly relevant data on specific aspects of the online debate that we can then analyze."

When they identified a potential manipulation campaign, staff members prepared a short detection report that listed the observations, and they then began work on a more detailed characterization report. This second document examined the details of the campaign, as detected, and tried to establish whether it was a foreign digital interference attempt as defined in the July 2021 decree that had created Viginum. To be characterized as such an attempt, a suspected campaign had to threaten France's fundamental interests, involve directly or indirectly a foreign state or nonstate entity, contain allegations that were manifestly inexact or deceptive, and intentionally use artificial or automated means to amplify its visibility.[19]

To justify such conclusions, Viginum needed customized tools for analyzing social media content. And with only a few months before the presidential election, the unit had no time to undertake a cumbersome public procurement procedure. Instead, Viginum worked with French companies already under contract with the government and designated by the Honfleur task force as viable suppliers of software for detecting disinformation.

"In July, when Viginum was created, we already had feedback from other institutions to guide us," Brillant said. Throughout the second half of 2021, Viginum's staff experimented with various tools and selected companies to develop technical solutions that matched the unit's specific needs. Viginum also developed tools internally, drawing on the talents of a dedicated team of data scientists in the operations department. The internally developed contributions included indicators to detect automated behavior on social media and interactive mapping systems that could identify information propagation patterns.

By the beginning of 2022, Viginum had defined its processes and was ready to begin efforts to protect the national election.

Defending the election

Protecting an election required the ability to work under an especially complex institutional arrangement. Election administration in a democratic society was supposed to be impartial in order to offer a level playing field for candidates and parties. Election management bodies had to work at arm's length from other parts of the executive branch or the legislature. But the greater the number of institutions involved and the more sensitive the communication and collaboration between them, the more difficult it might be to respond to crises.

"The importance of interpersonal relationships in high-pressure moments should not be overlooked," Brillant said. To build such relationships, in late January Viginum reached out to three partner institutions that shared responsibility for protecting the election. First was the National Commission for Control of the Electoral Campaign, organized for the presidential election and officially known as the Commission Nationale de Contrôle de la Campagne électorale en vue de l'Élection Présidentielle, which monitored various aspects of the campaign—such as public meetings, media coverage, and official campaign materials—and ensured that the state treated candidates equally. A new commission was created for each presidential election.

A second partner was the Constitutional Council (Conseil Constitutionnel), which supervised the ballot. It issued official results, ensured proper conduct and fairness, and made sure that candidates respected campaign spending limits. The council could declare an election invalid if conducted improperly.

The third was Arcom (Autorité de régulation de la communication audiovisuelle et numérique, or Regulatory Authority for Audiovisual and Digital Communication), which regulated both audiovisual and digital communications to ensure conformity with rules governing electoral campaigns.

"Before the campaign started, we met with all three election oversight bodies," said Brillant. "Once we all knew one another, it was easier to communicate." Viginum got together with the National Commission in February and the Constitutional Council a bit later and had several meetings with Arcom and the Ministry of the Interior's Elections Office. In addition, Viginum convened two meetings focused on election security, to which it invited the country's cybersecurity agency, Arcom, the government's Information Service, and the Elections Office.

In February, Viginum also began working to detect and characterize foreign digital interference campaigns, and throughout the election period, it sent to the three election oversight bodies reports describing the elements it had detected. "They sometimes asked additional questions to better understand the campaigns we were flagging," Brillant said. "We also reached out to them in April to schedule a hearing because we wanted to make sure they knew about specific information manipulation attempts." Throughout the process, Viginum also communicated with the country's cybersecurity agency to share thoughts about online activities it was noticing.

Civil society played an important role. In October 2021, the secretariat-general met with representatives from the main social media platforms in France. Ferriol and Brillant presented Viginum and its role, and the social media companies discussed their experiences with information manipulation in electoral settings and their strategies for fighting disinformation during the upcoming election. Viginum established direct lines of communication with the platforms, thereby enabling the unit to ask questions about specific campaigns, identify situations that required further discussion, and request that platforms flag suspicious incidents.

"Platforms paid close attention to information manipulation during the presidential election," Ferriol said. Viginum staff also relied on Objectif Désinfox, a fact-checking initiative set up by Agence France-Presse and Google and joined by many other media organizations. Viginum's staff used information from Objectif Désinfox to help characterize campaigns—notably, by checking whether content had been flagged as false or misleading.

Finally, the unit put in place ad hoc measures to prepare for high-pressure moments during the campaign. "We put an extended work schedule in place as well as on-call duty periods," said Benoit. Because no candidate won a majority on April 10, during the first ballot, a runoff was scheduled for April 24. Between the two dates, Macron and National Rally party candidate Marine Le Pen, Macron's main opponent, scheduled a televised debate. On the night of the debate, a dedicated team followed social media to make sure there was no foreign interference.

Days later, Macron won the election. Legislative elections followed in June. During the voting, Viginum staff members were on alert for significant information threats, but none emerged.

OVERCOMING OBSTACLES

Russia's invasion of Ukraine on February 24, 2022, injected an unexpected element of uncertainty into the 2022 French election. With just two months before the national vote, Viginum staffers immediately went on alert to keep watch for information manipulation attempts that were related to the conflict and could target France. "We got ready quickly. We had to determine the scope of the operation in a hurry because it was a priority," said Benoit.

Following a European Union–wide ban on Russian broadcasters Russia Today and Sputnik, Viginum kept a close eye on the way those outlets were trying to evade the order. According to Ferriol, the flexibility of Viginum's project-focused management model helped the unit organize quickly.

Counterintuitively, the invasion might have partly explained the lack of significant attacks on the French election. During the campaign period, Viginum characterized just five cases of foreign digital interference, and none was perceived to be serious enough to affect election integrity.

According to a report from the Online Election Integrity Watch Group—a group of nongovernmental organizations that analyzed disinformation during the French presidential election, "the war in Ukraine led to a redeployment of the resources of Russia, one of the main actors of foreign interference in the West. The ban of the Russian state-controlled media Sputnik and Russia Today (RT) from the major online platforms, and their focus on narratives to justify the war in Ukraine, weakened the ability of these outlets to influence people in France and diverted their attention from the French presidential campaign."[20]

"It is true that the war probably used up a lot of resources connected to Russian interests," Brillant said. "If services related to foreign interests were planning to target us before February 24, the war probably reoriented their efforts toward another priority, but it is mere speculation."

ASSESSING RESULTS

In 2022, Viginum detected 60 suspicious campaigns related to France's presidential and parliamentary elections. Its staff analyzed 12 campaigns in more detail and characterized 5 of them as foreign digital interference. Although the unit reported those five cases to the election oversight bodies, those institutions decided not to respond because they did not consider the threats urgent and massive. "When it comes to information, overreaction should be avoided," said Ferriol. "Campaign dynamics should dictate whether or not to react. If the campaign is running out of steam, reacting could [attract more attention to it and] end up reinforcing the adversary's narrative."

In its first annual report, Viginum revealed that it had detected suspicious online content on social media in March 2022 that implied the French government was using voting machines from Canadian–US firm Dominion Voting Systems Corporation in order to skew election results. The claims were getting traction on social media, and the unit alerted the Ministry of the Interior, which issued a public refutation. (The Ministry of the Interior was separate from the election oversight bodies—the National Commission for the Control of the Electoral Campaign, the Constitutional Council, and Arcom.)

Staff members also shared details of a second foreign interference campaign. In March 2022, Viginum detected dozens of suspicious accounts based in Africa that shared pro-Macron pictures mimicking the candidate's official campaign posters. Three days before the first round of the presidential election, an African media outlet revealed the existence of those accounts and accused the French president of using them as promotion tools. "This was actually a deliberate campaign with a clear narrative: implying that France was using troll farms based in Africa," said David Robert, head of Viginum's operations department. The unit shared information on the campaign with France's three election oversight bodies and the Operational Committee for Fighting Information Manipulation. The Operational Committee—which included representatives of the ministries of the Armed Forces, Foreign Affairs, and Interior—took measures to combat the attack.

In its own postelection review, the National Commission for Control of the Electoral Campaign, organized for the presidential election, concluded that the presidential campaign "did not face any significant events that could have affected its rollout."[21]

"Our job is to find gold nuggets," said Ferriol. "To find them, we have to sift a lot of sand. We spend a lot of time analyzing social media content. During the presidential and parliamentary elections, we had to examine 60 suspicious campaigns to find 5 that matched the definition of foreign digital interference. We have to remain humble, but I'm hoping that as we develop our expertise, our processes will become more efficient, and a higher share of our detections will be characterized as foreign interference."

REFLECTIONS

"In the future, information manipulation may be used not only by foreign states but also by criminal groups, which may benefit financially from disinformation," said Gabriel Ferriol, head of Viginum. In the face of such evolving threats, organizations such as Viginum would have to develop their expertise.

Ferriol described the challenge policy makers face in democratic societies. "The information threat is extraordinarily asymmetrical," he said. "Attackers can manipulate information remotely at relatively low cost, and they can target specific audiences and spread narratives with practically no risk." It was far more difficult for defenders to detect and deal with attacks carried on social media not only because of the multiplicity of platforms and the volume of communication but also because of the need to protect the free exchange of ideas and political debate in a democratic society.

Democratic governments were slowly assessing how best to proceed, taking one step at a time. They were learning from one another's experiments. By contrast with Viginum's policies, Sweden's Civil Contingencies Agency, which began dealing with disinformation threats in 2018, decided it would not monitor social media because it wanted to protect freedom of speech and what it perceived as the right to anonymity. (See companion ISS case study *Sweden Defends Its Elections against Disinformation, 2016 – 2018*.) Later, in 2022, Sweden launched the Swedish Psychological Defense Agency, its counterpart to Viginum. The agency's operations department described its mission as identifying, analyzing, and countering foreign malign information influence activities and other disinformation directed at Sweden or Swedish interests. "This includes producing reports and analysis relating to certain situations, threat actors, and societal vulnerabilities as well as proposing relevant countermeasures," the department said on its website. "In collaboration with other government agencies, the department also develops methods and technologies for identifying and countering foreign malign information influence activities."[22]

"France was able to put Viginum in place because the country had intellectually and juridically identified its fundamental interests," said Ferriol. "Partner countries ask us, 'How did you do it?' and I ask them, 'What do you want to protect?' If you are not able to explain to citizens what you are trying to protect within the online public debate, citizens will likely perceive your activity as threatening to civil liberties."

Viginum's strict mandate made the unit more acceptable to citizens of France.[23] Viginum could investigate suspicious activity only if the activity could affect fundamental interests, which were defined by law and included the nation's "independence, the integrity of its territory, its security, the republican form of its institutions, its means of defense and diplomacy, the safeguarding of its population in France and abroad, the balance of its natural surroundings and environment, and the essential elements of its scientific and economic potential and cultural heritage."

Although no major controversy emerged after Viginum's creation, Ferriol recognized that limited public understanding fueled narratives that depicted Viginum as a tool to discredit the government's political opponents.[24] During the electoral process, Viginum considered that it had a "duty of discretion," and it delegated to election oversight bodies the choice about whether to inform the public about disinformation campaigns it had detected.

Viginum released its first annual report in late October 2022. In a bid to enhance transparency, the report explained the agency's decision-making processes and disclosed the number of foreign interference efforts it had detected. However, the report neither provided *details* of the foreign interference attempts detected nor outlined subsequent actions, if any, taken by other agencies. Marc-Antoine Brillant, deputy head of Viginum, explained: "Viginum collects clues by using open-source intelligence. To accuse someone, you need proof, not just clues. Our reports provide a body of evidence that guides the work of competent authorities, which can then use additional techniques to find proof." Other competent bodies typically meant the Operational Committee for Fighting Information Manipulation, which included intelligence services.

Offering the correct degree of transparency posed a continuing challenge, however. "We are currently discussing the issue of transparency with Viginum," said Béatrice Bourgeois-Machureau, head of the Ethics and Scientific Committee. "To what extent can we communicate in order to provide the highest level of transparency for citizens while protecting elements that must remain confidential for the unit to work? That's a crucial element that we are working on."

References

[1] The Commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle (National Commission for Control of the Electoral Campaign for the Presidential Election) ensured that the state treated candidates equally during the electoral campaign. A new commission was established for each presidential election. Additional information can be found in the commission's 2017 final report: https://www.cnccep.fr/pdfs/CNCCEP-Rapport-final-2017.pdf

[2] https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf

[3] https://www.aa.com.tr/fr/monde/-notre-proph%C3%A8te-est-une-ligne-rouge-des-appels-arabes-%C3%A0-boycotter-la-france-/2018094

[4] https://www.europe1.fr/international/accusee-de-silence-la-turquie-condamne-lassassinat-monstrueux-de-samuel-paty-en-france-4001293

[5] See https://www.pure.ed.ac.uk/ws/portalfiles/portal/120126408/CraufurdSmithJML2019FakeNewsFrenchLaw.pdf or the law (in French): https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559

[6] https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law

[7] https://www.loc.gov/item/global-legal-monitor/2018-09-24/france-senate-rejects-fake-news-ban-bills/ and https://www.theguardian.com/world/2018/jun/07/france-macron-fake-news-law-criticised-parliament and https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law

[8] For instance, the Ministry of Armed Forces monitored informational risks in the context of military operations; the Ministry of the Interior developed tools in the fields of public safety and disorderly conduct; the Ministry of Foreign Affairs had started developing monitoring tools focusing on foreign policy; and Arcom monitored efforts from social media platforms to fight disinformation.

[9] See more information at https://www.gov.uk/government/publications/conflict-stability-and-security-fund-national-security-communications-team-programme-summary-2020-to-2021

[10] See more information at https://www.disinfo.eu/resources/spain-2/ in English and more details in Spanish at https://www.rtve.es/noticias/20201105/gobierno-plan-desinformacion-fake-news/2053203.shtml and at https://blogip.garrigues.com/publicidad/el-nuevo-procedimiento-de-actuacion-contra-la-desinformacion-la-polemica-esta-servida

[11] "The fundamental interests of the Nation [cover] its independence, the integrity of its territory, its security, the republican form of its institutions, its means of defense and diplomacy, the safeguarding of its population in France and abroad, the balance of its natural surroundings and environment, and the essential elements of its scientific and economic potential and cultural heritage." https://www.equalrightstrust.org/ertdocumentbank/french_penal_code_33.pdf

[12] The decree is available here : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043788361

[13] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044454840

[14] Although the Council of State's decisions are not publicly available, page 236 of the council's 2021 report gives additional information on this decision. See https://www.conseil-etat.fr/publications-colloques/rapports-d-activite/rapport-public-2021-des-juridictions-administratives

[15] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044454057

[16] https://www.welcometothejungle.com/fr/companies/viginum

[17] https://www.france24.com/en/americas/20211208-as-social-unrest-explodes-in-french-west-indies-chlordecone-is-key-to-the-crisis

[18] https://la1ere.francetvinfo.fr/nouvellecaledonie/referendum-en-nouvelle-caledonie-avec-une-tres-forte-abstention-le-non-l-emporte-pour-la-troisieme-fois-resultats-partiels-1178869.html

[19] This interpretation drew on the same passage of the law cited in note 11 in connection with Viginum's subject-matter focus. "The fundamental interests of the Nation [cover] its independence, the integrity of its territory, its security, the republican form of its institutions, its means of defense and diplomacy, the safeguarding of its population in France and abroad, the balance of its natural surroundings and environment, and the essential elements of its scientific and economic potential and cultural heritage." https://www.equalrightstrust.org/ertdocumentbank/french_penal_code_33.pdf

[20] See the report by the Institute for Strategic Dialogue (https://www.isdglobal.org/). The report appears at https://www.isdglobal.org/wp-content/uploads/2022/06/French-elections-report_Online-Election-Integrity-Watch-Group.pdf

[21] https://www.cnccep.fr/pdfs/CNCCEP-Rapport-final-2022.pdf

[22] https://www.mpf.se/en/about-us/

[23] French penal code article 410-1, French internal security code 811-3.

[24] One example can be found in the article at https://lecourrierdesstrateges.fr/2021/12/14/lagence-gouvernementale-viginum-pourra-surveiller-les-publications-des-francais-sur-les-reseaux-sociaux/