RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

VIGINUM

VIGINUM YEAR #1

Page 1

Preface

Page 2

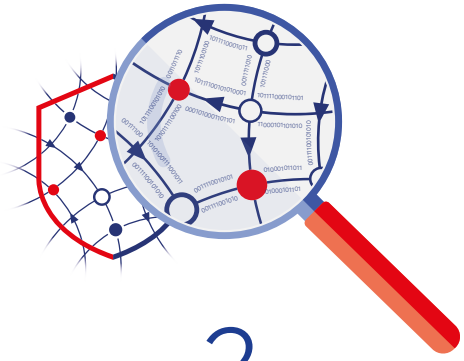
Key dates

Page 3

1

Legal and ethical framework

Page 11



2

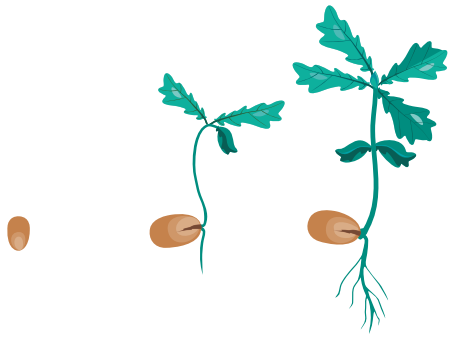
Operations

Page 19

3

The teams

Page 25



4

The ecosystem

Stéphane Bouillon,

Secretary-General for Defence and National Security

"There is always the risk of error and illusion in our perceptions"

Edgar Morin, *Lessons from a century of life.*

The newest of the Prime Minister's office within the General Secretariat for Defence and National Security, the service for vigilance and protection against foreign digital interference called VIGINUM, has celebrated its first year of existence on 14 July 2022. The time has therefore come to present the results of its first year of operation. Like any state entity, VIGINUM therefore reports on the performance of its duties not only to the parliamentary assemblies, but also to the supervisory bodies stipulated in the regulatory provisions organising and supervising its activities and under which the service has been created.

That is the purpose of this report.

It aims to honour the commitment to transparency that goes hand-in-hand with the service's mission. This commitment was made to the members of parliament and the bodies that were consulted at the preparation stage prior to the service's creation. Their comments were carefully considered to better meet the requirements of the conditions under which VIGINUM was going to operate.

These requirements undoubtedly stem from a widely shared awareness of the existence of concealed actors on online platforms, manipulating the visibility of chosen information and its reach and directing debates among Internet users using inauthentic processes, to harm our country's institutions, values and interests. Our national tradition is rooted in debates and rapid and sometimes passionate flows of ideas and information, and we can be proud of it. This is the hallmark of democracy. Unfortunately, our era is now also one of attempted manipulations and trickery, adversely affecting discussions on online platforms.

Drawing on the lessons of the recent past, France has availed itself of VIGINUM as the means to try to counter this trickery when it is organised from abroad. We all remember the foreign attempts to destabilise the 2017 presidential election known as the *Macronleaks*, or the attacks and defamation directed at our country after the murder of Samuel Paty on 16 October 2020. VIGINUM's role is to detect and characterise these artificial campaigns, involving foreign actors, aimed at misleading users of online platforms, twisting the accuracy of the democratic debate, including during elections, and in fact undermining France's fundamental interests. This field is both vast and well-defined. It must respect the rights of Internet users, their privacy, and our civil liberties. Safeguards must therefore be in place around all of VIGINUM's activities.

These are set out in the two decrees that form the basis of VIGINUM's work and constitute the solid framework within which it operates: the principles and terms were set in the decree establishing VIGINUM dated 13 July 2021, following lengthy consultation and in-depth legal work with the French Council of State. This process was supplemented by a demanding dialogue with the *Commission Nationale de l'Informatique et des Libertés* (France's data protection authority) and a review in the General Assembly of the French Council of State, which led to the publication of a second decree in December 2021 on the processing of the data collected.

In addition, for the sake of thoroughness, but also to anticipate future developments, it was decided to create an ethical and scientific committee which reports to me. This body comprises highly qualified persons in the legal, diplomatic, scientific and media fields. It carries out both supervisory and advisory functions and will, so I wish for the future, liaise with a talented, active and expert scientific community in the relevant fields of interest. I very much hope that this committee could also help us build dialogue with counterpart structures created in partner states, and with the European Union, which is taking a very active role in looking into foreign digital interference and disinformation.

VIGINUM has come a long way in its first year of existence. The path ahead of us is also a long one. VIGINUM's action is part of France's overall determination to continuously improve the protection of our fellow citizens against all those who wish to undermine our democracy and the fundamental values and interests of our country. Rest assured that all staff at the General Secretariat for Defence and National Security (SGDSN) are fully committed to this goal.

I hope that reading this report will convince you of this commitment.

KEY DATES

13 July 2021

Creation of VIGINUM under the General Secretariat for Defence and National Security (SGDSN), by decree no. 2021-922.

15 July 2021

Lieutenant-Colonel Marc-Antoine BRILLANT is appointed as Deputy Head of Service.

5 October 2021

Members of the ethical and scientific committee in charge of monitoring VIGINUM's activities appointed by order of the Prime Minister.

5 October 2021

Gabriel FERRIOL is appointed as Head of Service, reporting to the Secretary-General for Defence and National Security, by order of the Prime Minister.

9 September 2021

VIGINUM's presentation at the International Cybersecurity Forum (FIC).

11 October 2021

Meeting with the main digital platforms as part of the preparation for the 2022 French presidential election.

12 October 2021

Speech by the Secretary-General for Defence and National Security at the *Médias en Seine* festival.

13 October 2021

VIGINUM's presentation at the *"Démocratie et fait numérique: de l'information à l'action" (Democracy and digital fact: from information to action)* event organised by the *Conseil National du Numérique* in partnership with Inria and *Numérique en communs*.

10 November 2021

Inaugural meeting of the operational committee to combat information manipulation (interministerial network).

9 November 2021

Launch of the operation dedicated to securing the French presidential election from manipulation of information.

14 October 2021

Awareness-raising meeting for political parties in preparation for the 2022 presidential election.

26 November 2021

VIGINUM's presentation at the national "Science, Research and Society" forum.

7 December 2021

Automated processing of personal data instituted for the purpose of identifying foreign digital interference, by decree no. 2021-1587.

3 February 2022

VIGINUM's audition before the National Commission for Control of the Presidential Election Campaign (CNCCEP).

19 May 2022

VIGINUM's audition before the National Commission for Control of the Presidential Election Campaign (CNCCEP).

7 April 2022

VIGINUM's audition before the Constitutional Council.

18 February 2022

Awareness-raising meeting for campaign teams in preparation for the presidential election.

7 June 2022

VIGINUM's presentation at the OSINT day of the International Cyber Security Forum.

30 June 2022

VIGINUM's presentation at the *"Servir la France"* conference organised by the friends of the École de Guerre Économique.

13 July 2022

Celebration of VIGINUM's first anniversary.

Timeline of VIGINUM's operations p. 19.

1

LEGAL AND ETHICAL FRAMEWORK

Formed in the summer of 2021, VIGINUM is the national technical and operational service tasked with protecting digital public debate against information manipulation campaigns involving foreign actors intended to harm France and its fundamental interests. VIGINUM operates within a rigorous legal and ethical framework, based in particular on its permission to consult, collect and use personal data, and on the involvement of an ethical and scientific committee made up of highly qualified persons responsible for monitoring the conditions under which it fulfils its role.

The genesis of **VIGINUM**

Information manipulation is increasing and worsening

As part of what are known as "hybrid" competition, contestation or confrontation strategies, digital campaigns of information manipulation have become a key component in the international balance of power.

Such campaigns rely on a wide range of strategies and techniques with the aim of changing perceptions and altering collective behaviour. Their main objectives are to erode public trust in institutions, to polarise discussions on matters of general interest, and to create or amplify tensions within populations. They pose a serious threat to democratic societies that function on the basis of public debate, in this ultra-dynamic digital space, which has itself become a strategic theatre for states.

In recent years, more and more countries have disclosed that they have been victims of digital campaigns of information manipulation. These campaigns first appeared during election periods to influence voters or undermine the smooth running of the ballot, but they are now penetrating all areas of digital public debate, exploiting significant current events or social issues with the aim of twisting the accuracy of discussions or disrupting public order.

Over time, the threat has become more and more complicated to apprehend, whether one considers:

- the profiles of actors and sponsors (state or non-state actors, hierarchical or otherwise);
- their motives (planned operation or opportunistic exploitation of current events);
- their modus operandi (troll farms, bot networks, avatar animation, coordinated swarm-like attacks, building malicious narratives, dissemination of distorted or misleading information, postings within "echo chambers", etc.).

A number of states have decided to respond to this threat. While some have established inter-departmental or interministerial cooperation networks, others have opted for the creation of specialised structures tasked with providing protection against digital information manipulation campaigns involving foreign or domestic actors.

Many international institutions have also become involved. In 2015, within the European Union (EU), the European External Action Service (EEAS) created a Strategic Communication Division, "*StratCom*", supported by three regional *task forces* (East, South and Balkans) responsible for detecting digital information manipulation campaigns and designing appropriate counter-statements. Other international institutions (G7, OECD, etc.) have also taken up the challenge of combating information manipulation.

WHAT IS FOREIGN DIGITAL INTERFERENCE?

Foreign digital interference is an inauthentic phenomenon adversely affecting digital public debate and combining potential harm to France's fundamental interests, manifestly inaccurate or misleading content, massive and deliberate artificial or automated dissemination or intention to disseminate, and the direct or indirect involvement of a foreign actor (state, para-state or non-state).

France's response to information manipulation

In France, the threat posed by information manipulation, particularly in the democratic decision-making process, came to light during the "*Macron Leaks*" in 2017. On this occasion, the country had to face a digital information manipulation campaign, aimed at destabilising a candidate a few days before the second round of the presidential election. This included both a cyber component, with a computer attack resulting in the theft and leak of private data, and an informational component including the circulation of rumours and fake news.

As of 2018, the government took some initial measures to combat information manipulation by setting up an interministerial coordination network under the aegis of the SGDSN to better apprehend this new threat. At the same time, the French legislative arsenal was strengthened by the passing of law no. 2018-1202 regarding the fight against information manipulation on 22 December 2018, which endowed France's Audiovisual and Digital Communication Regulatory Authority (ARCOM) and interim relief judges with new prerogatives in this area.

THE CREATION OF VIGINUM FALLS WITHIN THE INCREASING USE OF SOCIAL MEDIA IN FRANCE.

In January 2021, France had 59.47 million internet users (up 2.5% in one year), of which 49.60 million used social media (up 13% in one year), i.e. 75.9% of the total population.

Source: Digital Report 2022 *(We are social/Hootsuite)*

In the autumn of 2020, the threat of information manipulation campaigns intensified. In the aftermath of the Islamist attack in Conflans-Sainte-Honorine, France was the target of a particularly virulent smear campaign on social media. In response, the executive decided to appoint the SGDSN to lead an interministerial working group, called the "Honfleur taskforce", responsible for investigating the dynamics of how anti-French discourse spreads on digital platforms and assessing its spontaneous character. The Honfleur taskforce ultimately concluded that a significant proportion of the sentiments expressed against France and its democratic model spread on social media were the result of inauthentic behaviour and information manipulation orchestrated by foreign actors.

This attempted destabilisation as well as the growing awareness of the threat have highlighted the need for France to strengthen its operational measures and tools to combat information manipulation.

A new **technical and operational service**

Decree no. 2021-922 of 13 July 2021

The decision to equip France with a specialised structure in charge of protection against information threats was taken at the beginning of 2021. An interim body, succeeding the Honfleur taskforce, was then set up.

Following preparatory work involving numerous political and parliamentary consultations, Decree no. 2021-922 of 13 July 2021 supplemented the existing provisions in the French Defence Code to give the Secretary-General for Defence and National Security new powers in the fight against information manipulation, and more particularly against foreign digital interference.

To assist the Secretary-General in exercising these new responsibilities, the decree created a service with national competence called the "Vigilance and Protection against Foreign Digital Interference Service", commonly known as VIGINUM.

This new technical and operational service is tasked with detecting and characterising, for the benefit of the SGDSN as well as the authorities responsible for the smooth running of national elections[1], any phenomena that meet the criteria for defining foreign digital interference as set forth in Decree no. 2021-922 of 13 July 2021:

- Involvement of foreign actor(s)
- Manifestly inaccurate or misleading content
- Fabricated amplification
- Harm to the French fundamental interests

As stated in Article 1 of Decree no. 2021-922 of 13 July 2021, the scope of VIGINUM's activity is limited to topics of digital public debate that affect France's fundamental interests, i.e. core matters of national sovereignty (e.g. independence, defence autonomy, territorial integrity, diplomacy and respect for international commitments, the functioning of institutions, the protection of major economic, industrial and scientific interests, etc.).

VIGINUM also supports the SGDSN in its role of coordinating interministerial work to combat information-related threats.
As part of its role, VIGINUM works with all the administrations contributing to the fight against information manipulation (Ministry of Europe and Foreign Affairs, Ministry of the Interior, Ministry of the Armed Forces, etc.). The service also contributes to European and international work in its field of activity, and maintains operational and/or technical relationships with its foreign counterparts, in compliance with the remit of the Ministry of Foreign Affairs.

For more information on the definition of VIGINUM's role: see Decree no. 2021-922 of 13 July 2021 creating VIGINUM, which sets out its missions.

1. During election periods, VIGINUM provides any useful information to a number of independent authorities and supervisory bodies such as the Audiovisual and Digital Communication Regulatory Authority (ARCOM) and the National Commission for Control of the Presidential Election Campaign (CNCCEP).

An ethical and scientific committee to oversee VIGINUM's activities

An ethical and scientific committee has been set up under the Secretary-General for Defence and National Security to oversee VIGINUM's activities. Its members include highly qualified persons in the diplomatic, legal, scientific and media fields. Since 15 October 2021, the ethical and scientific committee has been chaired by Béatrice BOURGEOIS-MACHUREAU, Councillor of State *(Conseil d'État)*. Its members are:

Béatrice Bourgeois-Machureau
Councillor of State (Conseil d'Etat) and Chair of the ethical and scientific committee

Jean-Maurice Ripert,
Ambassador of France

Benoît Loutrel,
Member of the ARCOM board

Pauline Talagrand, Deputy Editor-in-Chief of Digital Investigation at Agence France Presse (AFP)

Marie-Christine Tarrare,
Public prosecutor at the Besançon Court of Appeal

Aymeril Hoang,
Digital expert

Julie Joly,
MD at the weekly magazine L'*Obs*

Claude Kirchner,
Emeritus research director at INRIA (the National Institute for Research in Digital Science and Technology)

The ethical and scientific committee may be provided with all documents produced by VIGINUM. It is systematically informed of the start and end of operations conducted by VIGINUM. It receives regular information on the triggering and duration of any automated personal data collection initiated by the service. It receives all the analysis reports produced by VIGINUM. It may address recommendations to the Head of Service regarding the conditions under which VIGINUM fulfils its missions. The ethical and scientific committee produces an annual report, which is made public. Its chair submits the report to the Prime Minister.

The first annual report of the ethical and scientific committee will be published on the SGDSN website.

A strictly controlled automated process of personal data

Decree no. 2021-1587 of 7 December 2021

As part of its remit, VIGINUM carries out meticulous research and analysis work which involves examining publicly available information online. This information might include personal data for which the conditions of collecting, using and storing data are strictly regulated.

To carry out its role, VIGINUM is authorised to implement automated processing of personal data. The regulatory framework for such data processing was set by Decree no. 2021-1587 of 7 December 2021, issued after an opinion[2] from the French data protection authority (CNIL) and the French Council of State in general assembly.

The categories of personal data involved

Only certain categories of personal data can be collected in an automated manner by VIGINUM:

- identification data provided by the holders of accounts opened on online platforms;
- indicators to assess the activity and audience of these accounts (number of subscribers, number of posts, etc.);
- publicly accessible content published by account holders and associated audience indicators.

Access to personal data

Under the data processing framework governed by Decree no. 2021-1587 of 7 December 2021, VIGINUM is permitted access to publicly available personal data on digital platforms in two ways:

- as stipulated in Article 2 of the aforementioned Decree of 7 December 2021, the monitoring work consists of observing activity on online platforms, if necessary after logging on, without interacting with users. The regulatory framework provides that this monitoring activity does not entail automated collection of personal data. During such work, VIGINUM staff is allowed to manually collect personal data in order to establish the list of the technical criteria stipulated in the first paragraph of Article 2 of the Decree of 7 December 2021. They can also use publicly available data which are not of a personal nature (e.g. aggregated indicators such as volume, engagement, audience, etc.);

- as stipulated in Articles 1 to 4 of the aforementioned Decree of 7 December 2021, automated collection of personal data is performed on the basis of content publicly accessible to users of online platforms run by operators with activity on French territory in excess of five million unique visitors per month, including when access to these platforms requires registering an account. The selection of the data collected automatically is based on technical criteria, notably identified during the monitoring work.

VIGINUM does not collect content where access is subject to a prior re-

DEFINITIONS

Personal data means any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly. This can take the form of a name, a photo, an email address, an IP address, a login, etc.

Source: www.cnil.fr

Automated processing can be defined as any operation or set of operations carried out using an automated process (without human intervention).

Source: www.cnil.fr

2. Opinion no. 2021-116 of 07 October 2021.

RELATIONS WITH CNIL

CNIL is the French regulator responsible for ensuring the protection of personal data. In this capacity, it has the role of alerting, advising and informing all publics, and also has the power to control and sanction. VIGINUM maintains regular dialogue with CNIL's various departments in the framework of their respective roles.

quest or a login ratification step (for example, a closed group on a social media or on an instant messaging service).

In accordance with the provisions of Article 4 of Law no. 78-17 of 6 January 1978, which stipulates that automated collection of personal data must be "adequate", "relevant" and "non-excessive", the content to be collected is selected proportionately: automated collection of personal data is limited by technical criteria determined after monitoring work. The use of facial recognition or voice identification systems to select content is prohibited.

Content is collected for a maximum period of 7 days, renewable up to a maximum of six months from the date the collection was first initiated. Only agents individually authorised by the head of VIGINUM can access personal data collected by the service.

VIGINUM's automated collection of personal data is systematically reported to the ethical and scientific committee, which receives weekly reports on additions, deletions and changes to the technical criteria used for collection. As of 30 September 2022, VIGINUM has sent 87 such reports to the committee.

Storage and deletion of personal data

In accordance with Article 7 of the Decree of 7 December 2021, data collected automatically is stored only for the time strictly necessary for its analysis. They are deleted after being used, and in any event, no later than four months after the date of their collection, through an automated process.

In addition to its own IT tools and in compliance with the provisions of the aforementioned Decree no. 2021-1587, VIGINUM makes use of technical solutions provided by French and European service providers to fulfil its role.

Rights of data subjects

The processing of data, authorised by Decree no. 2021-1587 of 7 December 2021, constitutes a process related to state security and is therefore covered by Titles I and IV of French Law no. 78-17 of 6 January 1978 on data processing, data files and individual liberties. As such, data subjects have no right to object to such processing.

However, they may exercise their rights of access, rectification and erasure.

To ensure that these rights can be fully exercised, the Head of Service, who is the data controller, has appointed a data protection officer (DPO), who is responsible for responding to all requests made by any interested parties. The DPO's contact details and details of the procedure to follow are provided on the SGDSN website.

The right of access allows the data subject to obtain confirmation as to whether or not personal data concerning him or her are being processed. The right of rectification allows the data subject to obtain the rectification of inaccurate or incomplete personal data concerning him or her.
The right to erasure allows the data subject to obtain the erasure of personal data concerning him or her.

IN THE STAFF'S OWN WORDS

"As the data protection officer, my job is to ensure that data subjects can exercise their data protection rights. Through a dedicated email address, I am responsible for setting up a one-stop shop to collect and respond to all relevant requests of potential data subjects".

Organisational chart

SGDSN

VIGINUM

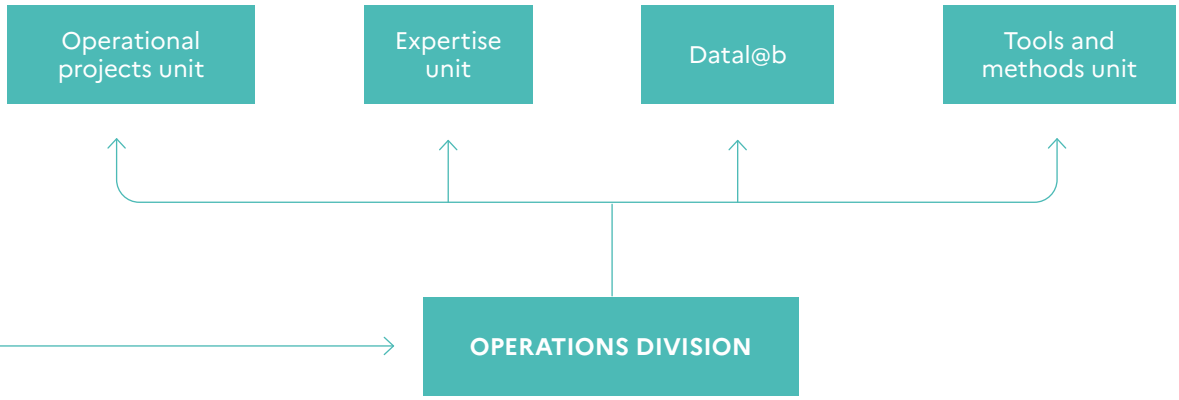
SGDSN

Decree no. 2021-922 of 13 July 2021 gave the Secretary-General for Defence and National Security new powers to combat foreign digital interference. Pursuant to subsection 9 of Article R-1132-3 of the French Defence Code, in liaison with the ministerial departments concerned, the Secretary-General for Defence and National Security "identifies operations directly or indirectly involving a foreign State or a foreign non-State entity with the intent of artificial or automated massive and deliberate dissemination, through an online public communication service, of allegations or accusations that are manifestly inaccurate or misleading and that are likely to undermine the fundamental interests of the Nation." The Secretary-General drives and coordinates interministerial work on protection against such operations.

Learn more: www.sgdsn.gouv.fr

VIGINUM'S MANAGEMENT

VIGINUM is a service with national competence, attached to the General Secretariat for Defence and National Security, responsible for vigilance and protection against foreign digital interference. The service is headed by a Head of Service assisted by a Deputy Head of Service.



The Operations Division is responsible for detecting inauthentic phenomena affecting digital public debate, and characterising those that meet the criteria defining foreign digital interference. It is home to specialists selected for their expertise in open source digital research and analysis, digital marketing, social media, political science, geopolitics and computer science. In particular, it includes a Datal@b, a team of expert data scientists tasked with improving the quantitative toolbox made available to VIGINUM's analysts.

COORDINATION AND STRATEGY UNIT

The Coordination and Strategy Unit drives interministerial coordination in countering information manipulation, assists the Operations Division in establishing and leading its operational cooperation, organises bilateral meetings with VIGINUM's foreign counterparts, contributes to determining France's stance on this topic in multilateral forums, and participates in multilateral work relating to the service's activities. It follows the work of the ethical and scientific committee attached to the SGDSN, for which it fills the secretarial function. It manages the service's internal and external communication policy, as well as the legal expertise related to VIGINUM's activities. It supports the Head of Service in implementing VIGINUM's strategy.

SUPPORT UNIT

Designed to provide VIGINUM's staff with optimal working conditions, the Support Unit is involved in managing human resources, finance, real estate, logistics, facilities, and secretarial services.

"A great collective adventure"

Gabriel Ferriol,
VIGINUM Head of Service

What challenges did VIGINUM face during its first year of existence?

This first year has been extremely fruitful. The service faced many challenges of many kinds, whether legal, methodological, HR or logistical, with major operational deadlines, in particular the elections of spring 2022.

What were your priorities in addressing those challenges?

We were faced with a large number of projects to be run within a very tight timeframe. There was a great risk of losing focus or becoming exhausted. To ward off that risk, I decided to mobilize the service on some straightforward priorities.

Firstly, it was essential to attract talent quickly to form hard core expertise in combating information manipulation. With these trailblazers, we built a clear methodological framework and a flexible organisation to deal with information threats. This structure has enabled us to adapt in an agile manner, even when we had to cope with unforeseen circumstances.
Secondly, in order to be understood and accepted, we needed to ensure that we were working within a clear and strict legal framework. Throughout the autumn of 2021, under the authority of the SGDSN, we worked to this end in conjunction with the CNIL and the French Council of State. This work, which led to the Decree of 7 December 2021, was essential to establish our legitimacy and demonstrate the objectivity of our approach.

And thirdly, we immediately started to work with a cooperative mindset. First of all, under the aegis of the SGDSN, interministerial collaboration with other departments involved in the fight against information manipulation. Secondly, institutional cooperation with the authorities responsible for the smooth running of national elections. Cooperation with the platforms too, from our respective roles, we held discussions with the shared goal of protecting digital public debate.

Expertise, objectivity and cooperation were the three watchwords for our work. These are the values that we convey on a daily basis.

What do you remember about this first year?

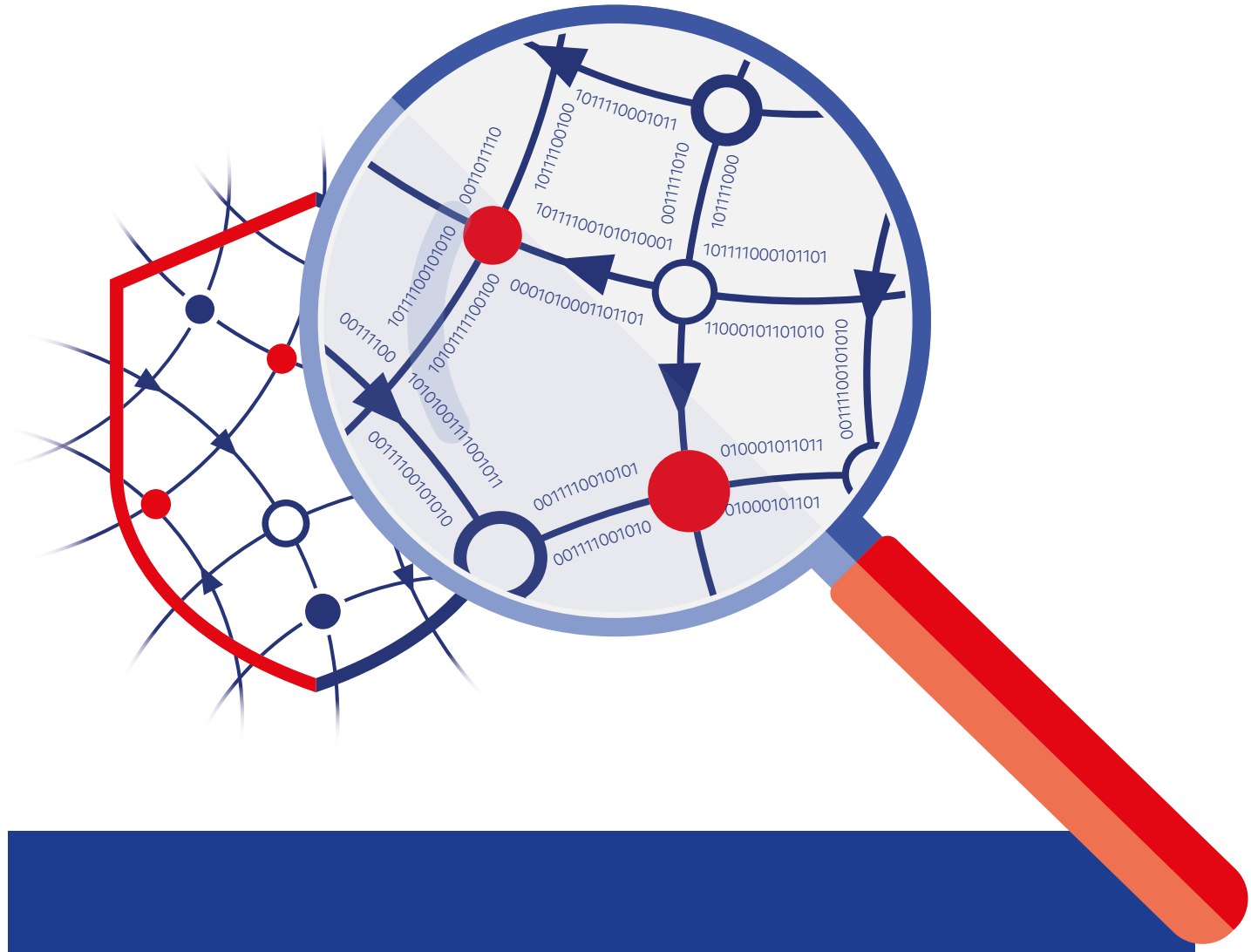
From this first year, I remember snapshots: moments of satisfaction, tension, doubt, joy or relief. Memorable moments, such as the weekends of autumn 2021 and spring 2021 when we secured the protection of the elections.

This first year of VIGINUM's existence has been a great collective adventure. I am extremely proud of the work done by VIGINUM's staff. The service's success is theirs above all, collectively.

I am also thinking of all those who, in other departments or other institutions, have accompanied us or facilitated our action. From the start, we were keen to be part of an ecosystem, to place ourselves at the service of others and to demonstrate our added value. We have managed to do this because of the warm welcome and the great support we have received.

What happens next?

Much remains to be done in the face of an ever-changing threat.
The adventure continues...



2

OPERATIONS

Detecting and characterising foreign digital interference is VIGINUM's core mission. The service had to meet several key operational deadlines in its first year of existence.

Detecting and characterising foreign digital interference

Detection work

Detection work consists of uncovering potentially inauthentic phenomena on online platforms that could indicate the presence of a foreign digital interference.

To uncover these phenomena, VIGINUM looks for markers of inauthenticity within digital public debate: atypical accounts, content likely to be inaccurate or misleading, and unusual, unexpected or coordinated behaviour. VIGINUM notably relies on mathematical indicators and IT tools designed by the data analysts of its Datal@b.

Characterisation work

Characterisation work consists of verifying whether or not the detected phenomena meet the criteria for defining foreign digital interference (see opposite). They may also aim to assess the potential purposes, the modus operandi and the actual, assumed or potential effects of these phenomena.

84
potentially inauthentic phenomena detected as of 22 July 2022.

How can foreign digital interference be characterised?

Involvement of foreign actor(s): identifying markers (technical, linguistic, semantic, behavioural) that reveal those involved are of foreign origin

Manifestly inaccurate or misleading content: highlighting manifestly inaccurate or misleading allegations or accusations, which can be objectively demonstrated to be false

Fabricated amplification: demonstrating that the dissemination of content is artificial or automated, large-scale and intentional

Harmful to France's fundamental interests: assessing the risk of harm to interests reaching the core of national sovereignty

IN THE STAFF'S OWN WORDS

"VIGINUM explores publicly accessible content online, on platforms, websites and web media, to detect and characterise foreign digital interference. VIGINUM staff are observers of the information landscape. We work in open source, without interacting with other users."

Targeted operations

What is an operation?

VIGINUM works by running a number of operations.

An operation covers a component of the digital public debate related to France's fundamental interests and for which a posture of vigilance is necessary in the face of a potential informational threat. The component could relate to institutional, diplomatic, economic, security, cultural or societal events, planned or unplanned, related to current events or unconnected, and either occurring in France or having an impact in France if they occur elsewhere. For example, a forthcoming nationwide election triggers the beginning of an operation.

A team of experts from the Operations Division, led by an Operation Project Manager (OPM), is assigned to each operation. This team is built specifically to respond to the threat, its context, its challenges and its intensity. It pools a range of expertise in digital research and analysis, data science and in the humanities, social and political sciences.

OPMs coordinate the work carried out by the teams under their responsibility. They coordinate and supervise implementation. They verify that the operation meets its requirements and objectives as well as its written

or oral restitution, according to the standards in force. During operations, OPMs have functional authority over team members. They report to the Head of the Operations Division.

The operations life cycle

The operations conducted by VIGINUM are of limited duration. More than one operation can run at the same time.

At the start of an operation, the dedicated team establishes the terms of reference for its work and determines its role and objectives. During this phase, VIGINUM's staff observes the public debate related to the subject matter of the operation. This observation period allows them to identify the relevant digital platforms and the technical criteria that will make for a successful investigation. Setting these terms of reference facilitates the subsequent detection and characterisation activities.

At the end of an operation, VIGINUM always conducts a feedback exercise designed to extract lessons from the operational experience, optimise the service's processes and methods, and improve its knowledge of how its "opponents" operate and its understanding of the information environment (platforms, tools, communities, etc.). This exercise also facilitates the sharing of lessons learned with the service's partners.

IN THE STAFF'S OWN WORDS

"The operation project manager is the person who frames an operation so that the team can understand the context of the work to be carried out. They also accompany, guide and support the team, like an orchestra conductor."

A first year **of varied operations**

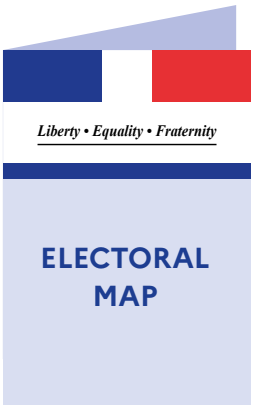
In its first year of existence, most of VIGINUM's operational activity was aimed at protecting the main election events, in particular the presidential and legislative elections of 2022. The service has also been active in protecting digital public debate in response to major international news events.

Keeping major elections secure in the information field.

As it has been noted during previous elections in France and abroad, election periods are peak times for foreign digital interference. Those manipulations of information can have various objectives: to sow confusion, uncertainty or mistrust among voters, to polarise the debate around divisive subjects and ideas, to fuel mistrust of mainstream media, or to discredit the institutions and the electoral process itself.

In September 2021, VIGINUM monitored French-language public debate about the German federal elections of 26 September 2021 to improve its knowledge of the issues that can be leveraged in national elections. In liaison with the competent German departments, VIGINUM's staff endeavoured to learn all the relevant lessons ready for upcoming French elections, particularly with regard to how to detect inauthentic behaviour and assess the seriousness of information threats during the election period (actors, subjects and operating methods).

From the beginning of October until 12 December 2021, VIGINUM conducted an operation designed to protect the digital public debate around the third referendum on New Caledonia's independence. The sensitive nature of this election, given the island's position in the Indo-Pacific area and current international tensions, necessitated the setting up of a continuous monitoring system designed to prevent any manipulation of information by foreign actors.



A few months later, the French presidential and legislative elections of 2022 were two major events for VIGINUM. From 9 November 2021 to 20 July 2022, the service's teams ran two successive operations aimed at keeping the April 2022 presidential election and the June 2022 general election as secure as possible in the information and digital field.

THE 2022 PRESIDENTIAL AND GENERAL ELECTIONS

Enhanced vigilance

From November 2021, VIGINUM started an operation to detect and characterise possible inauthentic phenomena adversely affecting the course of digital public debate around the 2022 presidential election.

In the course of its preparatory work, VIGINUM produced a detailed analysis on information threats against a background of elections, aimed at identifying those topics of public debate that are most vulnerable to information manipulation and at anticipating how actors are likely to operate.

From the date that the National Commission for Control of the Presidential Election Campaign (CNCCEP) was established, on 28 January 2022, VIGINUM has covered all the high spots of the presidential and general election campaigns (including on evenings and election weekends). During this period, the service sharpened its threat evaluation by detecting and characterising inauthentic behaviors that could be qualified as foreign digital interference.

An appropriate organisational structure

In view of its unprecedented scale, the operation to protect digital public debate around France's presidential election required wide-ranging adjustments to the service's internal functioning and organisation. An *ad-hoc* coordination centre was set up, to supervise various units focused on protecting candidates, monitoring key topics, and anticipating threats. Particular attention was paid to narratives that could undermine the credibility of the electoral process, both before and after the election. This organisational structure was extended, with some tweaks, for the 2022 general elections.

Consolidated synergies

VIGINUM reported any relevant information to the authorities responsible for the smooth running of the presidential election [3]. The Constitutional Council, the National Commission for Control of the Presidential Election Campaign (CNCCEP), and the Audiovisual and Digital Communication Regulatory Authority (ARCOM) were consequently recipients of all the service's analysis. Exchanges between VIGINUM and these authorities then continued in the context of the general elections. Afterwards, as part of collecting feedback, VIGINUM gathered the observations of these authorities ensuring the smooth running of elections so as to incorporate them into an overall assessment of its operational role during the election period.

During the election period, VIGINUM also intensified its exchanges with other agencies with operational capacities in the fight against information manipulation. Contacts have moreover been established with the major digital platforms.

SOME KEY FIGURES

In the course of its operations to protect the digital public debate surrounding the 2022 presidential and general elections, VIGINUM detected:

60
inauthentic phenomena on digital platforms.

12
were thoroughly investigated for characterisation purposes.

5
were finally characterised as meeting the criteria defining foreign digital interference.

3. In accordance with the provisions of the subsection of Article 3 of Decree no. 2021-922 of 13 July 2021.

"Protecting the digital public debate around the election"

Lieutenant-Colonel **Marc-Antoine Brillant,**

Deputy Head of Service at VIGINUM, in charge of the 2022 presidential election security operation

What is the threat status during an election period?

Since the mid-2010s, a growing number of democratic countries have been subject to foreign digital interference campaigns on social networks and media during major elections. The aim of those perpetrating these information threats is to modify perceptions, to in turn alter the behaviour of certain groups of people, with the main consequence of undermining the fairness of the election or the conditions under which the vote is being held.

In an electoral context, foreign digital interference can be aimed either at promoting or denigrating a candidate or a party, or at polarising the debate on certain issues, or at fuelling mainstream media distrust or at discrediting the institutions and the electoral process itself.

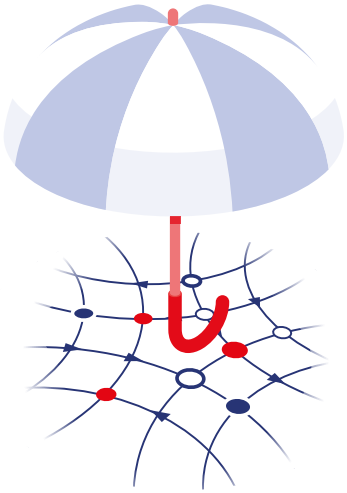
From November 2021 onwards, we focused on threat analysis, with the first challenge being to gain a thorough understanding of the various modus operandi that have been documented during overseas elections, including identity theft, deliberate data leakage, amplification of negative narratives, outsourcing *via* the use of private structures or active communities on platforms to conduct foreign digital interference, and the targeting of small but highly active audiences in terms of online engagement.

Do you have a concrete example of foreign digital interference during the French presidential election campaign?

In the 2020 US presidential election, several North American activists accused the Canadian company *"Dominion Voting System"* of involvement in orchestrated electoral fraud against the incumbent President Donald Trump.

Between 9 and 20 March 2022, VIGINUM observed the rapid spread of manifestly inaccurate or misleading content (writing, images, videos), across several social media platforms, mentioning the alleged use, by the French government, of voting machines from the Canadian company, with the aim of falsifying the presidential election. Before this manipulation of information gained any serious momentum, the French Ministry of the Interior and several media outlets quickly dismissed this false information.

PROTECTING DIGITAL PUBLIC DEBATE IN THE LIGHT OF CURRENT EVENTS



VIGINUM's role is to protect all issues of digital public debate that affect France's fundamental interests. This scope is not limited to major elections; it encompasses a wide range of interests including territorial integrity and national defence, foreign policy, implementation of France's European and international commitments, key economic, industrial and scientific interests, and so on.

During its first year of activity, VIGINUM conducted numerous operations to protect digital public debate around various national or international news events that could be exploited by malicious foreign actors, such as the war in Ukraine or France's involvement in the Sahel.

THE WAR IN UKRAINE

Whether it is a question of convincing public opinion that intervention is legitimate, or countering the real or supposed influence of an adversary, manipulation of information has become an integral part of military manoeuvring.

Given its diplomatic commitment to the Ukrainian issue and the French presidency of the Council of the European Union during the first half of 2022, France has emerged as a primary target for possible information manipulation campaigns orchestrated by foreign actors in the context of the conflict in Ukraine.

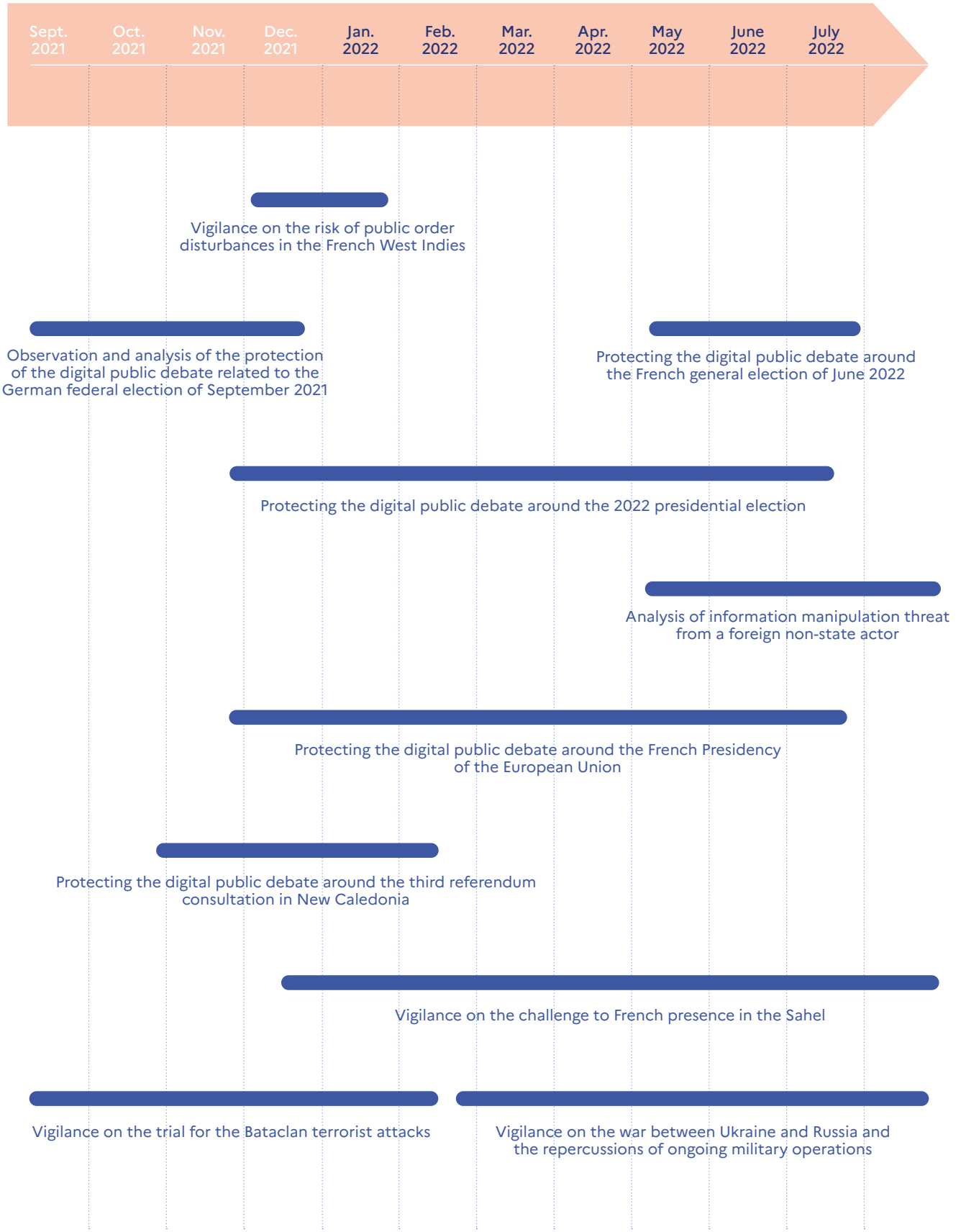
On day one of the military conflict, VIGINUM therefore started a specific operation to protect the digital public debate around the war in Ukraine in order to be able to detect and characterise any manipulation of information designed to discredit, delegitimise, destabilise or smear French institutions and/or fundamental interests.

FRENCH MILITARY ENGAGEMENT IN THE SAHEL

During the period 2021-2022, relations between France and Mali deteriorated sharply, as was shown by events such as the announcement of the reorganisation of the Barkhane operation, the suspension of the France 24 and RFI TV channels in Mali and the expulsion of the French ambassador in Bamako.

As the paramilitary group Wagner has been deployed in Mali since late 2021, this deterioration has created fertile ground for digital campaigns of manipulation of information that may target France. Therefore, in close collaboration with interministerial cooperation bodies involved in the fight against information manipulation, VIGINUM launched an operation to protect the digital public debate surrounding France's action in the Sahel.

OPERATIONS TIMELINE YEAR#1



"A collaborative and agile organisation"

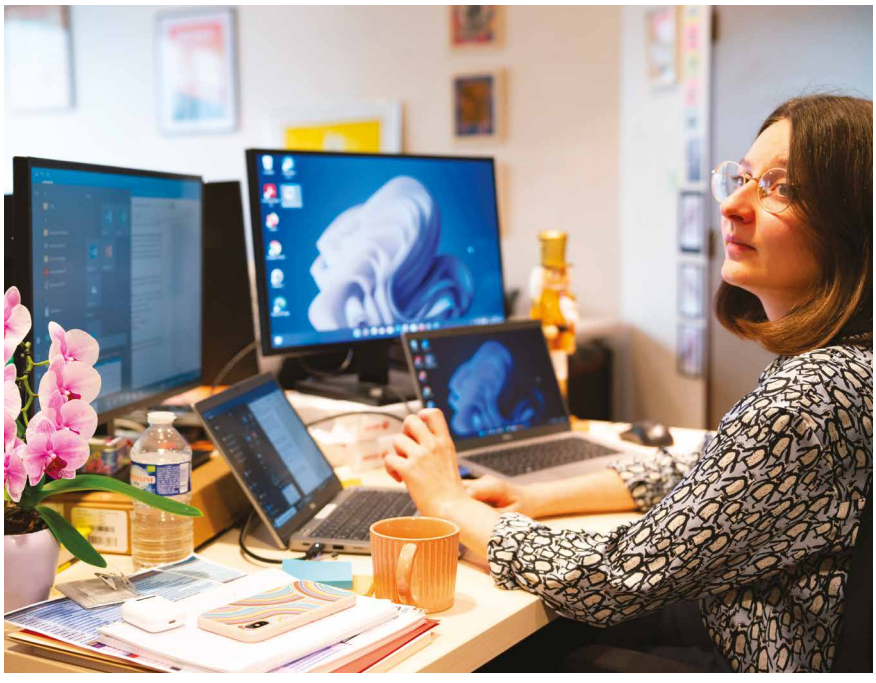
David Robert,
Head of the Operations Division

How was the Operations Division organised during its first year of existence?

When VIGINUM was created, the Operations Division's main objective was to be able to quickly set up multi-disciplinary operational teams, regardless of the operations' areas of focus.

To achieve this objective, we chose to run the Operations Division as an agile organisation in which resources and staff are not rigidly assigned individually to predetermined activities, geographical areas or specific subjects.

VIGINUM's Operations Division is in fact a flexible group of staff made up of analysts with highly specialised and complementary skills (specialists in digital investigation and analysis, digital *marketing*, political science and geopolitics, experts in data science, IT, etc.). This approach allowed VIGINUM to cover more than one operation in parallel and to react quickly to national and especially international events.



By working together, staff members learn from each other's methods, discuss ideas and develop new ways of detecting foreign digital interference. In other words, they inspire each other and continue to develop their skills.

What are the next challenges for the Operations Division?

We have initiated a number of structuring projects that we will continue to pursue, including the welcoming of new members, paying particular attention to their integration. We will also continue to develop synergies between our talents in the Expertise Unit and in the Datal@b, in particular to meet operational requirements effectively. We will also endeavour to put our technical and operational procedures on a more formal footing, and to capitalise on our knowledge and professionalise our expertise to ensure it endures.

3

THE TEAMS

The fulfilment of VIGINUM's role relies above all on the collective expertise of its staff and the individual commitment of its agents.

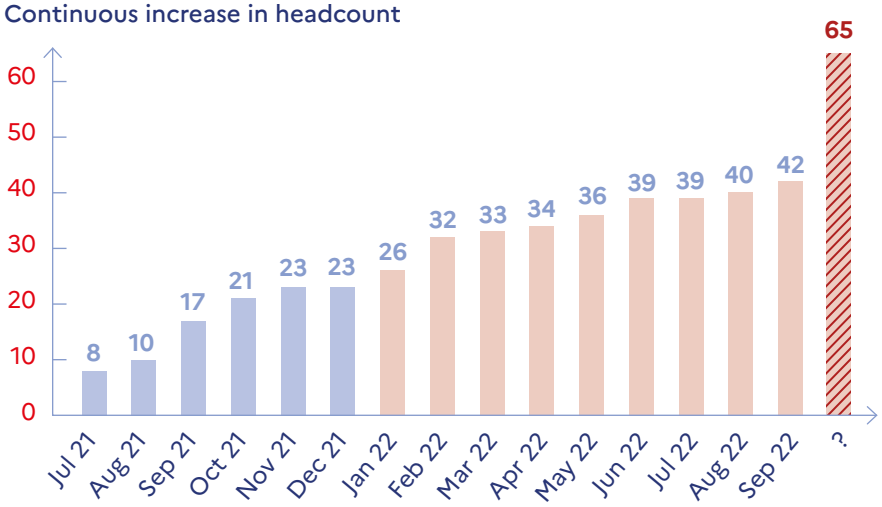
The ramping up of VIGINUM

A first year with plenty of recruitment

For a service under development, with nationwide competence, such as VIGINUM, recruitment is a major challenge in the first year of operation. From 13 July 2021 to 30 September 2022, more than 40 members of staff joined VIGINUM.
VIGINUM's recruitment strategy aimed to build a set of staff bringing together all the skills required for the smooth running of the service: specialists in digital investigation and analysis (OSINT), web and digital marketing professionals, data science experts, information systems engineers, political science and geopolitics specialists, support staff, senior managers and operational staff.
In terms of their status, VIGINUM members of staff include civil servants from the Prime Minister's services, permanent public servants from other ministries who are made available to the service, as well as numerous contractual agents.

To continue to attract the best talents against a backdrop of ever-expanding digital professions, VIGINUM is actively pursuing its recruitment campaign. As of 30 September 2022, the service is two-thirds of the way through its ramping-up trajectory. VIGINUM's headcount is expected to eventually reach 65.

Continuous increase in headcount



Training and support

To optimise its staff's performance and fulfil its role as effectively as possible, VIGINUM allocates significant resources to supporting the professional development of its agents, including through training.

In its first year of existence, VIGINUM has consequently built a programme to develop and increase its workforce's skills and enhance their potential and expertise. This programme includes training courses, organised both internally and by external providers, covering a wide range of skills and tools: monitoring toolkits, OSINT investigation tools and methods, cartography training, learning programming languages, foreign language courses, etc.

As the head of the Expertise Unit summarises, this is *"based on operations' needs but also on a longer-term vision, we must understand and anticipate teams' training needs. The service's objective now is to extend the training effort by actively involving staff in defining their career paths. Our aim is to place skills management at the heart of our work."*

42 people

72% working on operations

60% women

34 average age

90% of category A positions

2/3 under contracts governed by public law

Figures as of 30 September 2022.

“Recruitment, a major challenge”

Ludivine Le Douarin,

HR/recruitment representative

What is the strength of VIGINUM today?

VIGINUM’s role is carried out by a multi-disciplinary collection of experts in digital investigation and analysis (OSINT), digital marketing, data science, political science and geopolitics. This set of people is responsible for the detection and characterisation of foreign digital interference. VIGINUM’s support function units are home to staff with varied skillsets (HR, legal, compliance, communication, coordination, etc.).

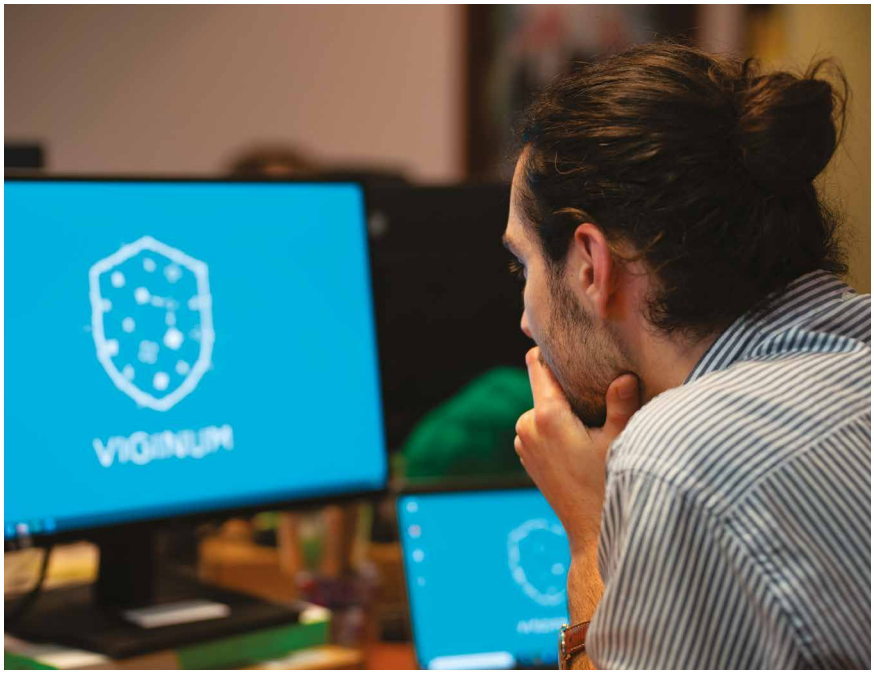
From the private or public sector backgrounds, young graduates or experienced, our agents have very different but complementary career paths and expertise, to which they add each and every day by sharing knowledge and learning from each other. It is the combination of these profiles and expertise that gives the service its strength and VIGINUM’s added value.

What were the most sought-after profiles over this first year of existence?

Over the past year, VIGINUM’s recruitment efforts have focused on ramping up the Operations Division, the core of VIGINUM’s operational reactor. The aim was to develop the Expertise Unit and the Datal@b, which are composed of analysts and data scientists.

To promote our professions and our work environment, we collaborated with the recruitment media “*Welcome to the Jungle*”. We are also present on LinkedIn and regularly publish our job offers and news. In addition, some members of the service travel to schools and training centres to meet potential future members of staff.

Finally, thanks to its discussions with its partners in the governmental sector, VIGINUM is working to develop an agile recruitment policy able to encourage interministerial careers and mobility, including by taking on seconded staff.



Working environment and **cohesion**

Working environment

From the time it moved into its Paris premises in July 2021, VIGINUM has been committed to promoting a pleasant and collaborative working environment while providing its staff with the resources and tools necessary to fulfil their missions.

Cohesion

To strengthen team spirit and a sense of belonging, particular attention was paid to the staff induction process and their well-being in the workplace. A well-being in the workplace survey has been designed in the form of a questionnaire submitted to staff every six months.

Along the same lines, VIGINUM promotes, through its internal communication, healthy circulation of information and knowledge sharing.

Budget

VIGINUM is a service with nationwide competence attached to the General Secretariat for Defence and National Security, within the Prime Minister's Office. The budget allocated to remunerate its staff, cover its operating costs and undertake its investment operations are ringfenced by budgetary programme 129 *Coordination of Government Work*, within the *Government actions directorate plan*. They are managed by the SGDSN's General Administration Service (SAG).

Visual identity

The design and production of VIGINUM's visual identity were key projects during the service's first year of existence in order to bind the team and give meaning to its actions. The service used a design professional to ensure the project's success. VIGINUM consequently has its own visual identity, in line with the guidelines set by the state's branding.

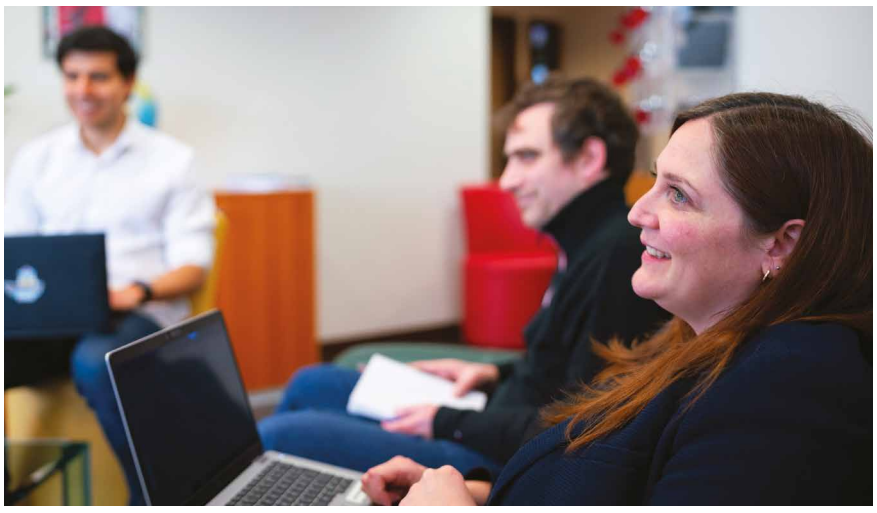
The VIGINUM logo explained

The challenge was to symbolise VIGINUM's role in a modern way, while at the same time emphasising the national dimension of its work. Several symbols were selected:
• Stylized outline of France to delimit the scope of the service's work;
• the colours (red, white and blue) to underline the national character of the mission;

VIGINUM
VIGILANCE AND PROTECTION AGAINST FOREIGN DIGITAL INTERFERENCE

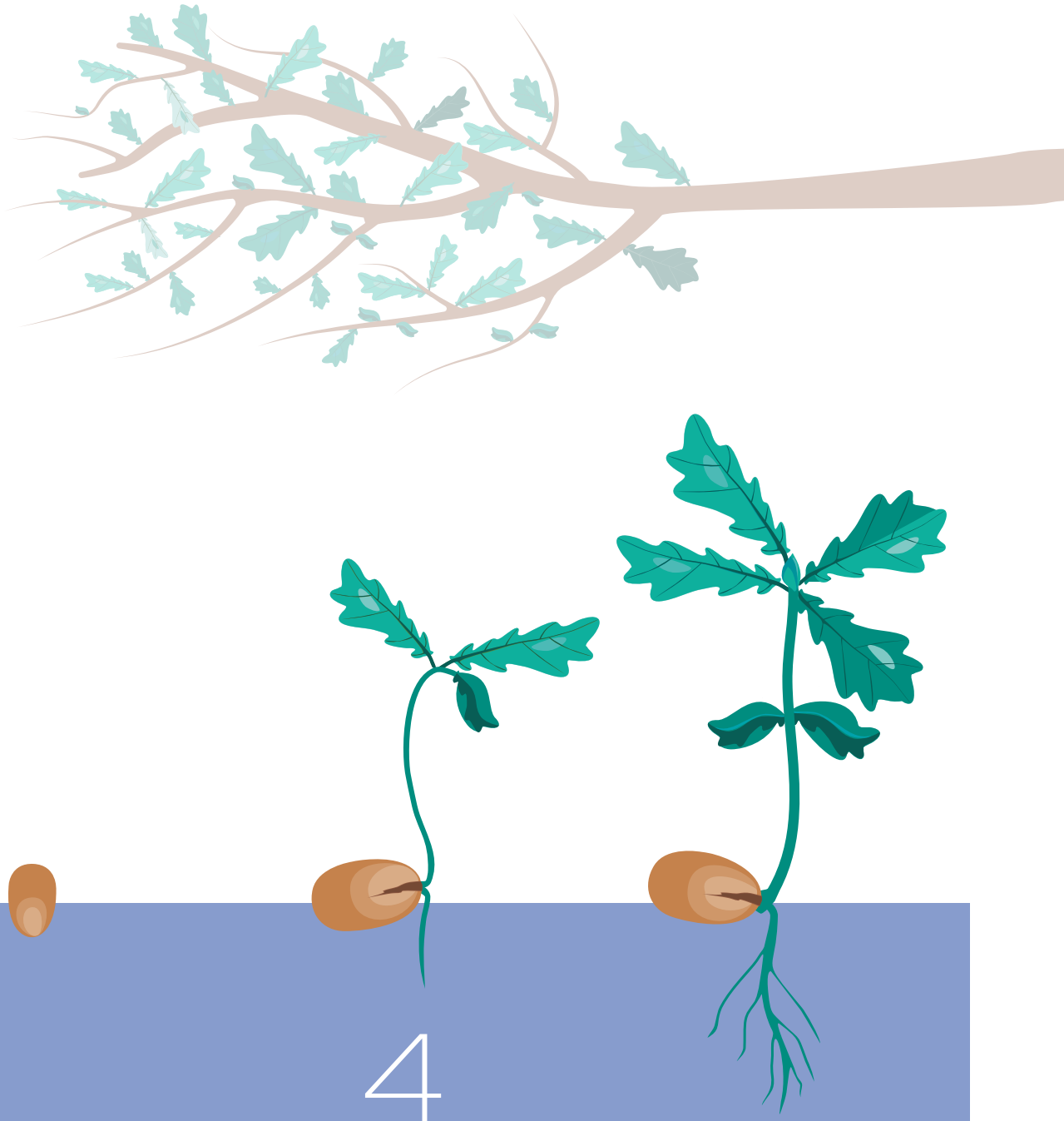
• the shield to embody protection;
• networks and dynamics of spreading across the country from outside to symbolise external information manipulation threats;
• the signature, "vigilance and protection against foreign digital interference" to ensure the service's missions are clear and understandable.

VIGINUM's style guide sets out how to use the logo and frames the form of all the services' productions.



VIGINUM'S 1st ANNIVERSARY

There are events that remain in the memory of a service. In July 2022, VIGINUM celebrated its first anniversary. To mark the occasion and celebrate collectively the results obtained in securing the elections, the service invited its interministerial partners to come together for a social event.



4

THE ECOSYSTEM

VIGINUM is not alone in the fight against foreign digital interference. Its work is part of a more comprehensive national and international ecosystem working to combat information manipulation. Within this ecosystem, VIGINUM interacts permanently with all the stakeholders who contribute, each in their own field, to meeting the many challenges posed by the information manipulation threat. The service accordingly works closely with other French administrations and services contributing to the fight against manipulation of information. It maintains close relations with certain independent authorities, such as ARCOM. It is developing relations with foreign partners and also aims to establish regular contacts with specialists in the academic sphere.

An **essential** interministerial coordination

As part of its operational activities, VIGINUM works closely with other administrations and services contributing to the fight against information manipulation: Prime Minister's administrations, entities within the Ministry for Europe and Foreign Affairs, the Ministry of the Interior, and the Ministry of the Armed Forces, etc.

A number of cooperation networks have been created to ensure smooth and responsive exchange of information, coordination at the technical level, as well as a consistent approach to information manipulation threats. These networks are established at different levels:

At the technical level: coordinated by VIGINUM, the monitoring, detection, characterisation and proposal network ("VDC-P") brings together administrations able to provide technical capabilities to counter information manipulation. The exchanges are operational, technical or methodological in nature.

At the operational level; chaired by the SGDSN, the operational committee for combating information manipulation brings together management from services with operational capabilities and their reporting authorities and representatives from the ministerial offices concerned. The committee's tasks include formulating working guidelines in the fight against manipulation of information as well as response proposals, for the attention of higher authorities, in the event of characterised foreign digital interference. VIGINUM implements the working guidelines set by the operational committee and coordinates accordingly the work of the VDC-P network.

In addition to these technical and operational interministerial networks, VIGINUM maintains partnerships with other administrations and services. In May 2022, VIGINUM signed an agreement with PEReN (center of expertise in digital regulation), a service with nationwide competence providing data science expertise to all state administrations on the subject of regulation of digital platforms. This agreement sets the terms governing the assistance provided by PEReN to VIGINUM on designing tools and studies useful to the service's missions.

Claire Benoit,

Head of VIGINUM's Coordination and Strategy Unit

Who were the main contacts during this first year of activity of the service?

The information manipulation threat is changeable and multi-faceted. It can be approached from different angles: operational, political, geopolitical, scientific or legal. To meet the challenges that the service had to face during this first year of its construction, VIGINUM has focused its external relations on supporting its operational activities.

The priority was to develop and coordinate interministerial technical and operational cooperation involving all the administrations participating in the fight against manipulation of information. Indeed, while VIGINUM works exclusively on publicly accessible data, other state services have complementary resources to enrich the analysis of risk phenomena. Interministerial cooperation is essential to better prevent and respond effectively to the threat.

At the same time, in the context of its operation related to the protection of the French presidential election, the service exchanged with the major digital platforms, that welcomed its creation. VIGINUM also met with European and international stakeholders to benefit from their operational experience.

What do you think is the right approach to effectively combat digital information manipulation campaigns?

Only a comprehensive approach will be effective in combating digital information manipulation campaigns. This is why VIGINUM wishes to intensify its relations with the stakeholders of this ecosystem. The service has therefore set itself a priority objective of developing its relationships with the academic world in the coming months.

European and international cooperation **to be encouraged**

Many states and international organisations are concerned about better protecting themselves against digital information manipulation campaigns. As information manipulation threat becomes more global, close European and international cooperation is more necessary than ever.

In coordination with the SGDSN and the Ministry of Europe and Foreign Affairs, VIGINUM has made initial bilateral contacts among several of its foreign counterparts, in Europe or in democracies regularly targeted by campaigns of information manipulation. Those states most directly exposed to the threat or with expertise in the field were prioritised. The service was thus able to benefit from various operational experiences and to compare the French approach with that of other countries. For the German federal elections on 26 September 2021, VIGINUM set up collaboration with the German services in charge of monitoring and protecting this election. A joint operational approach was initiated with the twofold objective of monitoring French-speaking public debate about the German election and preparing France a few months ahead of its own major elections.

In general, the international stakeholders with which VIGINUM has talked have shown a strong interest in the service's creation. They were particularly interested in the legal and ethical framework put in place to supervise and monitor its functioning. Topics of common interest were also discussed, such as protecting electoral processes and sharing good practices.

In coordination with the SGDSN and the ministries concerned, VIGINUM also helps determine France's position on the fight against information manipulation in multilateral fora. VIGINUM contributes to the discussions of various international working groups dealing with combating disinformation set up by the European External Action Service (EEAS) as well as those of the Horizontal Working Party on *"Enhancing Resilience and Countering Hybrid Threats"* attached to the Council of the European Union.

Similarly, in its first year of operation, VIGINUM has participated in international technical workshops on combating information manipulation. These workshops enabled VIGINUM's staff to exchange views with their counterparts on common operational issues, compare methodologies and share good practices. In this regard, the service is following the work of the G7 *Rapid Response Mechanism* initiative (set up by the Canadian G7 Presidency in 2018), which is working to identify measures and best practices against foreign disinformation.

Lutz Güllner, Head of StratCom at the European External Action Service

"With the creation of VIGINUM, France has shown the way forward with a dedicated structure to address information manipulation and foreign digital interference as a security issue. At the European level, we are delighted to be able to count on this twin structure to explore the avenues of cooperation which are open to us."

Interactions with **platforms**

In addition to public-sector stakeholders, the successful fulfilment of VIGINUM's role requires relationships to be built with private-sector stakeholders such as digital platforms. The latter occupy a central place in the ecosystem to combat manipulation of information. In its first year of operation, the service has established contacts among the major digital platforms, which have welcomed its creation. Discussions focused on the operational issues related to keeping the presidential election secure.

In addition to the platforms, VIGINUM maintains contacts with industry players whose technologies are likely to contribute positively to the achieving of its objectives.

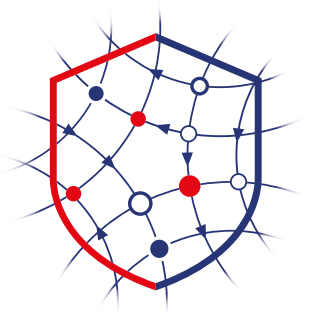
Establishing collaboration with the **academic sphere**

The issue of information manipulation is currently the subject of a great deal of academic and scientific work, carried out by a multi-disciplinary and highly committed community (including universities, specialised institutions and study centres, research centres, research laboratories, foundations and *think-tanks*). For a technical service such as VIGINUM, dialogue with this community is essential to build concepts, understand phenomena and educate experts.

This is why the service is committed to active collaboration with the academic world, the contribution from which is crucial.

On 26 November 2021, for example, VIGINUM took part in the *"National Forum on Science, Research and Society"* organised by the French Ministry of Higher Education, Research and Innovation. This event was an opportunity to meet researchers and to collectively discuss the challenges of the fight against information manipulation.

After these initial contacts, VIGINUM will aim, in the coming months, to build links with various actors in the academic sphere. More generally, VIGINUM remains attentive to academic debates and initiatives from the civil society involved in the global reflection on the fight against information manipulation.



VIGINUM

VIGILANCE AND
PROTECTION AGAINST
FOREIGN DIGITAL
INTERFERENCE

Published by VIGINUM,
Vigilance and Protection against Foreign Digital
Interference Service

Head of Publication: Gabriel Ferriol
Project management: Laura B
Editorial coordination and writing: Laura B
Graphics coordination: Clémence Picart
Design and production: Marion Raffaitin |
www.marionraffaitin.com
Photo credits: Patrick Gaillardin / SGDSN
Illustrations: Marion Raffaitin
Printing: SGDSN

ABOUT VIGINUM

Created on 13 July 2021 and attached to the SGDSN (General Secretariat for Defence and National Security), VIGINUM is tasked with protecting France and its interests against foreign digital interference.
The role of this national technical and operational service is to detect and characterise information manipulation that involve foreign actors and aims at harming France and its fundamental interests.

www.sgdsn.gouv.fr/viginum