



GOVERNEMENT

*Liberté
Égalité
Fraternité*



NATIONAL INTELLIGENCE STRATEGY

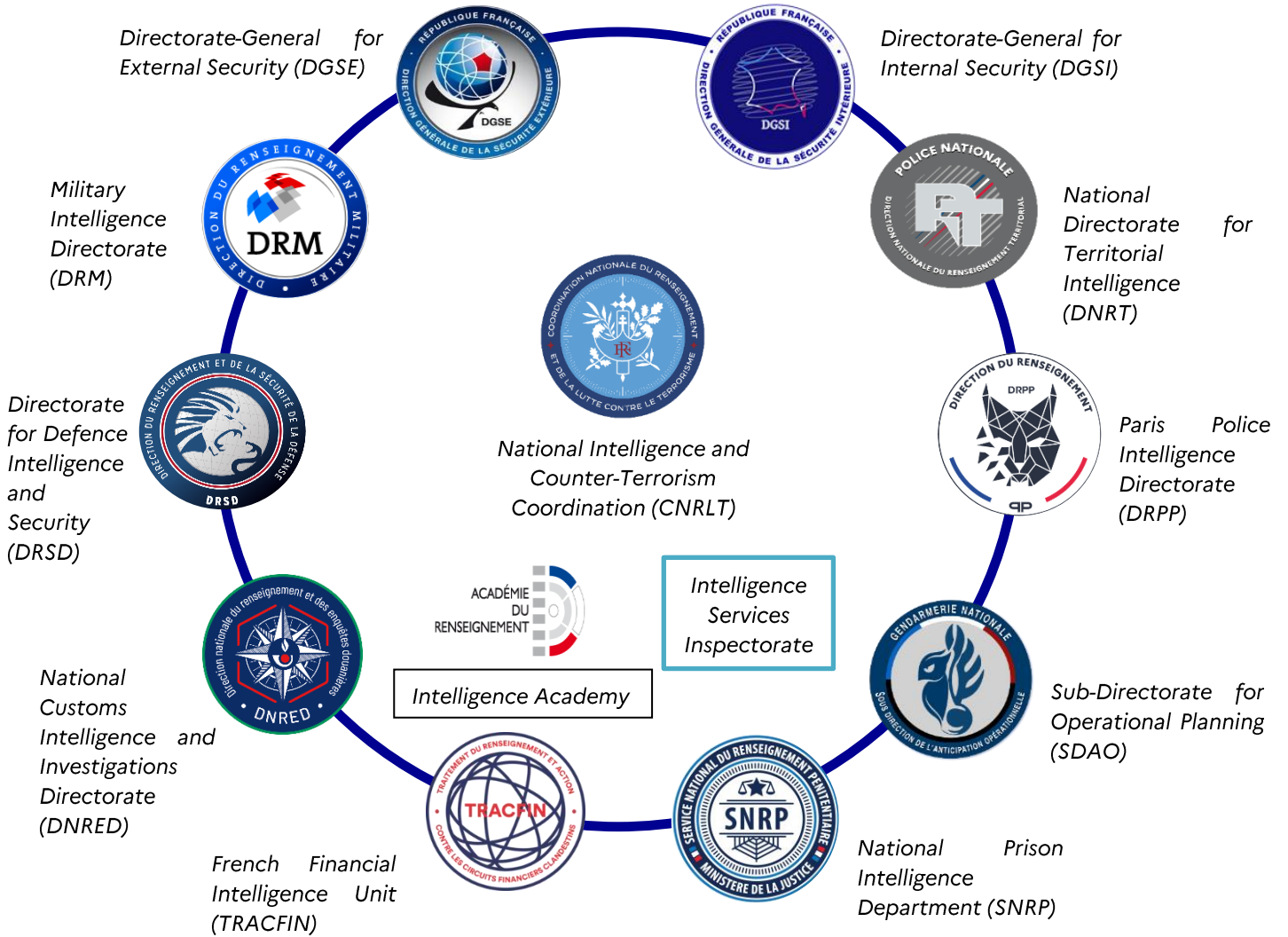


National Intelligence and Counter-Terrorism Coordination
January 2025

NATIONAL INTELLIGENCE STRATEGY

The intelligence community	4
What is the public intelligence policy?	5
Foreword by the Coordinator	6
PILLAR 1: Understanding global developments and preparing for strategic challenges	7
PILLAR 2: Intelligence for decision-making and action	13
PILLAR 3: Sharing, cooperating and working for our security in France, in Europe and worldwide ...	19
PILLAR 4: Intelligence within the rule of law	25
PILLAR 5: Harnessing all the necessary technologies for intelligence activities	31
PILLAR 6: Attracting and promoting skills in the French intelligence.....	37

The intelligence community



Intelligence refers to an activity that consists in gathering, cross-checking and analysing strategic information to inform decision-making by government authorities and disrupt threats. *Intelligence* is therefore the product of these activities performed by dedicated public structures called *intelligence services*. Their action is designed to protect France's sovereignty and institutions from threats and risks at home and abroad and to protect and promote the Nation's fundamental interests. Transformative changes have been made to the organization of the intelligence activities in the last 30 years to forge a *public intelligence policy* capable of meeting the democratic needs and the oversight of the state authorities, the parliament and the judicial authorities:

- In 1991, the Act of 10 July on the secrecy of correspondence establishing the National Committee for Security Interception Oversight;
- In 2007, the Act of 9 October creating the Parliamentary Intelligence Delegation;
- In 2008, with the White Paper on Security and National Defence and the creation of the National Intelligence Coordination (CNR);
- In 2015, the French Intelligence Act of 24 July.

In 2017, the President of the French Republic took forward these developments by scaling up the services' human and technical resources now reinforced each fiscal year with pluriannual policy acts coordinated and implemented by the ministers in charge of the intelligence services: *Ministre d'État*, Minister of Justice, *Ministre d'État*, Minister of the Interior; Minister for the Economy, Finance and Industrial and Digital Sovereignty; Minister for the Armed Forces; and Minister for Public Accounts.

Henceforth, the services benefit from a stronger coordination body in the form of the National Intelligence and Counter-Terrorism Coordination (CNRLT), which succeeded the CNR in 2017. The CNRLT has a mandate to develop and update the national intelligence plans and intelligence doctrines. It ensures that the government authorities receive the intelligence produced by the services and coordinates cooperation between the ten services of the national intelligence community. It is also tasked with promoting the intelligence community's priorities in interministerial discussions, in particular with respect to human resources, legal developments and pooled technical capabilities.

The drafting of this third National Intelligence Strategy is part of a full-fledged public intelligence policy embodied by its heads of service, steered by their supervisory ministers with CNRLT coordination, and overseen by Parliament and by independent administrative authorities.

In 2019, the National Intelligence Strategy drew the due consequences of an environment marked by four priority challenges: the terrorist threat, the anticipation of disruptive crises and risks, either for national security or international order, the protection and promotion of our economy, and the cross-cutting threats (such as cyber, interference, espionage, organized crime and the proliferation of weapons of mass destruction). The community was to take up these challenges by carrying out its missions and by anticipating developments in terms of human resources, service guidelines and relations with partners.

The 2022 National Strategic Review pointed out the key contribution provided by the intelligence services to the strategic “anticipation/knowledge” function, which it extended to “understanding” since government authorities need a sound understanding of the phenomena at work, to be able to plan and make decisions.

New strategic disruptions are underway, as with Russia’s invasion of Ukraine, illustrating the return of high-intensity conflicts in Europe. Amid this global context of international relations deregulation, with a threat of espionage stronger than ever, France is confronted on its own territory, with a proliferation of destabilization operations and violent acts, conducted or masterminded by hostile powers’ intelligence services. The threat of Islamist terrorism runs as high as ever and finds a new international echo chamber with the resurgence of the Israeli-Palestinian conflict following the 7th October 2023 attacks by Hamas and the many hotspots in the Middle East. In addition, the information revolution in the age of social media and mass information exposes us to information saturation and information manipulation by France’s adversaries. As far as domestic security is concerned, the Nation’s fundamental interests are threatened by extremist and separatist ideologies embodied by sectarianism, unrest and violent acts. France is faced, alongside its partners, with the major risks of organized crime, and particularly of drug trafficking, exposing our societies in terms of security, institutional destabilization and public health.

In this environment, intelligence is both tested and more decisive than ever. Our course never wavers: to guarantee our decision-making autonomy, to disrupt threats and to take action in France and abroad for our national sovereignty and European solidarity within the rule of law. It has to adapt constantly to hold this course steady, by seeking out the best skills and by using the most appropriate technologies. The environment calls for deeper dialogue with academics, experts and civil society as a whole, to better understand the global disruptions, to anticipate technological shocks and to prepare together how to tackle threats France is facing.

It was instrumental to update the National Intelligence Strategy in response to the new global and national environment. As the single unclassified strategic document of the national intelligence community, the strategy intends to share the analyses and the ambitions of the 20,000 committed and passionate women and men who are the national intelligence community.

Pascal MAILHOS, Prefect,

National Intelligence and Counter-Terrorism Coordinator

PILLAR 1:

Understanding
global developments
and preparing
for strategic challenges

1.1. Analyse the deterioration in the strategic environment

The strategic environment is marked by a deterioration in the international balances, going on for a number of years and by strong tensions on national territory. Globally speaking, an increasing rivalry between powers is to be observed, including in shared space (such as cyber, space and seabed), the return of high-intensity warfare in Europe combined with the use of nuclear rhetoric, and the persistence of a global terrorist threat. France is affected directly and indirectly by these exogenous dynamics, not to mention ideological radicalization. National cohesion is also being eroded by separatist ideologies promoting segregation and religious sectarianism.

1.1.1 International situation: an obvious weakening of global balances

- **Persistence of global threats**

Governments are collectively confronted with structural challenges such as organized crime, climate change, pandemics such as COVID-19 and the proliferation of weapons of mass destruction.

Terrorism remains a singularly significant challenge considering the ongoing risks associated particularly with Islamism, which offshoots are constantly morphing and restructuring. New hotspots of terrorist organization activity have been identified worldwide and are being closely monitored.

- **Unbridled economic competition**

The world's leading powers are engaged in economic competition that exploits the laws and violates the rules of international trade. France is responding with a strategy to protect and promote its economic, financial, industrial and technological sovereignty and regain its economic attractiveness. The intelligence services work alongside national business entities to protect business from destabilization attempts, technology and know-how capture, economic predation, unfair competition and lawfare. Economic and financial security awareness campaigns help all kind of French businesses to adjust to these challenges.

- **From espionage to the development of hybrid strategies**

Strategic competitors constantly diversify and improve their modus operandi, combining traditional espionage with cyberattacks and new forms of interference and influence (information manipulation, criminal group manipulation, sabotage, etc.).

The intelligence services work on the front line to detect and disrupt these concealed strategies and activities, maintained below the threshold of military intervention.

Services striving for economic sovereignty

The intelligence services contribute to France's economic sovereignty by detecting and neutralizing threats potentially targeting French economic, financial and scientific interests.

With their action aligned with the «France 2023 Plan», a €54-billion investment plan announced by the President of the French Republic in 2021, the intelligence services protect daily French strategic assets, businesses and laboratories in an increased competitive environment. Support to promote our economy is the second track of the services' economic intelligence action. Furthermore, the intelligence services contribute to counter public finances fraud.

The return of war in Europe

The large-scale invasion of Ukraine by Russia in February 2022 marks the continued illegal and now-unbridled use of force and aggressive strategies by global and regional powers.

Following the terrorist attack on Israel by Hamas on 7th October 2023, the resurgence of the Israeli-Palestinian conflict underscores this increase, in the frequency and intensity, of armed conflicts. It is indicative of the factors of instability throughout the region from Yemen – where terrorist group activities impact on merchant shipping in the Red Sea – to Iran even as they undermine the stability of the Levant, particularly Lebanon and Syria. The protracted nature of this degeneration in the situation inevitably has repercussions for our national security, and the intelligence services keep a close eye on developments in this area.

- **Unrestrained use of force and intensification of armed conflicts**

The large-scale invasion of Ukraine by Russia in February 2022 marks the continued illegal and now-unbridled use of force and of aggressive strategies by global and regional powers.

Following the terrorist attack on Israel by Hamas on 7th October 2023, the resurgence of the Israeli-Palestinian conflict underscores this increase, in the frequency and intensity, of armed conflicts. It is indicative of the factors of instability throughout the region from Yemen – where terrorist group activities impact on merchant shipping in the Red Sea – to Iran even as they undermine the stability of the Levant, particularly Lebanon and Syria. The protracted nature of this degeneration in the situation inevitably has repercussions for our national security, and the intelligence services keep a close eye on developments in this area.

1.12. National situation: the French society tackling with violent extremism and separatist ideologies

France has to face outbreaks of fierce protest (2018-2019 yellow jackets movement, protests and major urban violence such as in the summer of 2023) and the action of extremist groups that reject the Republican and democratic forms of expression in favour of violent radical actions.

The growing number of assaults on elected officials and the sharp rise in anti-Semitic acts are the increasingly visible symptoms of concerning tensions in French society.

Moreover, the terrorist threat level remains high in France as in other Western countries. From now on, it is driven by both well-identified profiles (individuals with a long history of radicalization, convicted and would-be terrorists, and radicalized individuals with mental health issues) and by individuals who are younger and younger. Several attacks and foiled plots in the last two years were perpetrated by minors, including preadolescents, capable of committing extremely violent acts.

11.3. The information revolution, common denominator of those crisis

The information society is defined by an acceleration and an exponential growth of the disseminated contents, particularly thanks to social media. This situation creates an illusion of greater transparency, but it also enables hostile state actors and business entities, as well as criminal and terrorist networks, to target France by distributing manipulated information. Faced with these emerging threats, the intelligence services are introducing in their areas of responsibility, new sophisticated search and fact-checking tools, as well as information analysis and rapid response procedures.

12. Anticipation of future challenges

The “knowledge, understanding and anticipation” strategic function is the intelligence services’ core mission. This means gathering information that can be used to anticipate events, including the least probable, especially when their impacts could threaten national security or affect the life of the Nation.

12.1. Identification of emerging threats

The intensification of crises, risks and threats is a structural dynamic. The two-folded challenge for the intelligence community is to identify emerging threats that will drive future crises and respond to them. Major technological innovations, terrorist and criminal groups’ adaptation and innovation strategies, and the growth and acceleration in the speed of the circulation of flows (human, financial, etc.) due to globalization will have strategic, political, economic, financial and social repercussions that need to be anticipated to provide government authorities with the relevant intelligence to make informed political decisions.

12.2. Scaling up dialogue between the intelligence community and experts

The intelligence community’s work with academic and research communities, think tanks, civil society and the private sector will be taken forward and scaled up to leverage all the resources needed to collectively understand risks and threats. This work must contribute to the training of agents and the organization of the services to ensure that it is fully taken on board by the intelligence community.

The intelligence community aims to work more closely with academia. The goal is to improve the understanding and anticipation of strategic challenges, with each actor in his respective area of responsibility and with his professional and ethical standards.

Foreign interference and information manipulation: threats to democracy

Intelligence is key in countering foreign interference operations in the information environment. Such operations are designed to distort the reality and manipulate international crises and democratic processes while undermining our political systems and our national cohesion. The intelligence services work alongside the General Secretariat for Defence and National Security (SGDSN), and its Service for Vigilance and Protection against Foreign Digital Interference (VIGINUM), to detect and assess information attacks against France, including by gathering information for potential attribution. They are authorized to respond to such attacks if needs be.

Response to a still-high terrorist threat

Resolute action by the intelligence and counter-terrorism services has foiled numerous attacks on the national territory since 2014:

81 Islamist attacks (including 52 since 2017);

13 extreme far right attacks;

1 extreme far left attack;

1 state-inspired attack.

In the face of a constantly evolving threat, the services need to constantly adapt, refocus their detection techniques, readjust the mechanism and choose the right counter measure at the appropriate time.

They therefore work together on the Permanent Staff (EMAP) made up of 12 intelligence and counter-terrorism services to ensure the intelligence-investigation continuum in liaison with the National Counter-Terrorism Prosecutor's Office.



PILLAR 2:

Intelligence for
decision-making and
action

21. Adapting to information saturation and crisis acceleration

The acceleration and interconnection of crises along with the risk of information saturation mean that the services need to be able to prioritize and disseminate intelligence. They therefore need the capability to monitor and analyse a growing number of issues and crisis zones.

22. Informing decision-making by authorities in a complex environment

Intelligence must provide decisionmakers with an informed appreciation of the strategic context of the international order and of the national situation, ahead of decisions regarding the Nation's fundamental interests or the security of our nationals. As a traditional intelligence mission, support for decision-making aims therefore at providing government authorities with reliable, relevant, up-to-date and exclusive information, according to set priorities. Each service, under the authority of its supervisory minister, produces strategic input designed to inform decisions. The National Intelligence and Counter-Terrorism Coordination (CNRLT) plays a coordination and briefing role to ensure daily that the government authorities have the most relevant intelligence and that analytical standards are maintained at a high level throughout the community in the long run.

23. Detecting and disrupt threats

Threat disruption represents the ability to prevent, as a matter of priority, the manifestation of a threat or, failing its prevention, to put an end to it. This can take a number of forms: legal, military, political, diplomatic, trade, financial, cyber, information and administrative. The disruption mission is an integral part of intelligence, whether conducted directly by services with disruption capabilities or based on elements gathered by the intelligence services. Disruption concerns, in particular, countering terrorism and violent extremism. The measures taken have delivered significant results in preventing attacks and violent actions and prosecuting their perpetrators. Disruption also counters other threats, some of which can be cross-cutting, including, in particular, proliferation of weapons of mass destruction, proliferation of conventional weapons, espionage and interference, predatory economic and financial practices and technology capture, cyberattacks, organized crime, unlawful immigration, separatism, and sectarian aberrations.

24. Intelligence for our armed forces

Outside the national territory, military intelligence provided to the armed forces consists in assessing the capabilities and possibilities for action (or the intent) of armed forces and armed groups that could harm our interests. This intelligence also assesses armament programmes, our competitors' innovative capacities, the morale of their defence and security forces, and the soundness of their partners. This wide range of intelligence is required to

implement the national defence policy.

Military intelligence also enables the armed forces to plan and carry out operations and cover all areas of conflict. Intelligence precedes military action – there can be no military operation without intelligence.

Increased disruption of espionage

The threat of espionage by foreign intelligence services has never been dispelled and remains acute. Espionage is generally carried out by intelligence officers operating on our territory under diplomatic cover. A total of 53 of these foreign intelligence officers have been expelled from France over the last ten years due to their activities in violation of the Vienna Convention.

Prevent acts of violence

Intelligence precedes decisions and intelligence precedes action. A recent example of this is Operation Sagittarius.

In April 2023, the security situation in Sudan suddenly deteriorated. The security of French nationals was threatened by violent fighting between the regular army and a paramilitary group. With an ongoing assessment of the risk level, meticulous monitoring of the fast-evolving tactical situation and a selection of options for action, French intelligence worked on providing the President of the French Republic, the Minister for the Armed Forces and the Chief of the Defence Staff with the accurate and cross-checked information they needed to make a sovereign assessment of the situation. The decision was made to plan and then launch an evacuation operation. This was the start of Operation Sagittarius.

The intelligence provided to the armed forces engaged in this operation gave them detailed knowledge of the environment and the belligerents, enabling them to safely evacuate 936 people in an extremely difficult situation.

The evacuees included 224 French nationals, but also 39 other European, African, American and Asian nationalities. More than a year after the operation and in the light of the current security situation in Sudan, our assessment of the situation at the time was clearly relevant.

Contribution of intelligence to holding the Paris 2024 Olympic Games

Combined work by the intelligence services, with a large number of police forces on the streets, proved highly effective. The forward planning for the event with dedicated structures, implemented two years in advance and a centralized, coordinated working methodology underpinned by a steadfast commitment, helped prevent any terrorist or violent actions.

An international cooperation centre hosted liaison officers from numerous partner countries in the summer of 2024 to share the collected intelligence and work together to mitigate the threats.

25. Scale-up in the complementarity and cooperation between services

Intelligence works according to certain modus operandi (confidentiality, intelligence-gathering techniques, etc.) and a high level of interservice coordination.

All the services' priorities in this area are laid down in the National Intelligence Orientation Plan (PNOR) as the first step in the intelligence cycle (steer, gather, analyse/exploit and disseminate) in a coordinated approach. This classified document organises, in a coherent manner, intelligence gathering, while remaining open to adaptation in the event of unforeseen circumstances.

Intelligence doctrines roll out the pillars of the PNOR to address major threats identified, such as counter-terrorism.

This hierarchized body of policy papers (the PNOR and the intelligence doctrines) establishes the strategy, assigns operational responsibilities to the different services, and limits the risks of duplication and dead ends.

The CNRLT regularly updates these documents in liaison with the ten intelligence services and reports on them to the state authorities.

26. Contributing to the protection of public finances

In a context where public finances are a key issue, and with them the ability to provide a high level of funding for public services and social security, the fair contribution of each and every individual is absolutely essential. The perception of the extent of financial, tax and social security fraud is particularly unacceptable to our fellow citizens. By contributing to countering public finances fraud, the intelligence services make an essential contribution to the smooth running of the country and to the national cohesion.

Prevent organized crime

Prevention of organized crime is one of the seven purposes of intelligence service action as defined by the law and, as such, tackles what has been identified from the outset as prejudicial to the Nation's fundamental interests. Drug trafficking, the number one global criminal market, represents a growing national security threat. This is an observation shared at the European level: massive scale of illegal drug flows and associated money laundering networks, growth in trafficking, corruption, criminal violence, and now direct assaults on the rule of law.

Yet, organized crime is not restricted to drug trafficking. It covers a vast range of offences such as arms trafficking, human trafficking, organized crime support to illegal residents, serious economic and financial fraud, organized theft and robbery, environmental crime, etc.

In this context a full mobilization of the intelligence services in support of the judicial investigations is needed.

Supporting our foreign policy

Our diplomatic network works in over 150 countries, with the support – among others – of information and analyses provided by the intelligence services. The use of information, obtained by sovereign means or with the help of our partners and allies, aims at enabling our diplomatic network to meet the challenges of shifts in balances of power and the proliferation of regional crises, including the protection of French nationals abroad.

The intelligence services' focus on global issues is essential to enable our diplomatic network to take effective action, including in managing the impact of globalisation and in addressing environmental change.

PILLAR 3:

Sharing,
cooperating and
working for our security
in France, in Europe and
worldwide

The threats impacting our societies play out at different levels (Pillar 1). Terrorism is as much a geopolitical reality as it is an endogenous threat. Violent extremism can take root locally even as it becomes embedded in global ideologies. Hostile powers can be tempted to work with criminal organizations. To fulfil its missions in this deteriorated environment (Pillar 2), the intelligence community has shared principles of organization:

- **Cohesion:** Each threat corresponds to an interservice chain of responsibility;
- **Suitability:** Organizations need to use the right tools for each level of action (local, national and international);
- **Decomartmentalization:** Information sharing between services is a systematic goal for the development of operational synergies, within security clearance rules and the need to know.

3.1. At the local level, detecting and disrupting violent, criminal and interference activities

The intelligence community is responsible for identifying and reporting on the emergence of societal phenomena and attacks on the values of the Nation, the population and its interests. The intelligence services therefore work on the ground gathering, centralizing and analysing information in all areas that could disturb public order (terrorism, collective or individual violent actions).

Working along the same lines as in counter-terrorism, the services work under the authority of the prefects and public prosecutors and use administrative, investigative, security, economic and financial tools to mitigate the threat.

Particularly close attention is paid to French overseas territories to tackle the difficulties they encounter (prevalence of trafficking, undocumented immigration networks and attempted interference by hostile powers) and safeguard their strategic assets.

3.2. At the national level, being ready to respond to each threat

Each intelligence community service is responsible for security in its field of competence. Local and national steering ensure that all threats are handled by lead services and support services (including other security forces but also public and private institutions, academia and think tanks).

The objective is to build a security continuum to combine in a coherent manner all the services' competences in action strategies using all the available tools.

Detect radicalization trajectories

Set up in 2014, the local organization for the prevention of terrorist radicalization takes a dual approach for a holistic and consistent appreciation of actions:

“Security/intelligence” (the *Département* Assessment Group);

“Prevention” (the *Département* Monitoring Unit for the Prevention of Radicalization and Support for Families).

The *département* prefect (local representative of the state authority) regularly holds meetings of these bodies with the participation of local players, including the public prosecutor. Their activity is sustained at the national level by the intelligence services.

Since 2020, the system was reinforced to take into account and counter separatist movements in various structures (associations, companies, shops, sports clubs, etc.) with the creation of local unit: *Département* Counter-Islamism and Counter-Sectarianism Units (CLIR).

Criminal intelligence: an example of the development of complementarity between services

Standing as an illustration of the security continuum, the prevention of organized crime is one of the remits of French intelligence in liaison with the criminal investigation services. This partnership is implemented in particular in countering drug trafficking and migrant smuggling networks. Coordinated by two criminal investigation services – the Anti-Narcotics Office (OFAST) and the Office for Combating Migrant Smuggling (OLTIM) – countering these crimes fully includes intelligence in a synergy of investigative and administrative counter measures.



3.3. Response to transnational threats with an information-sharing and cooperation strategy with our foreign counterparts

Although France has an autonomous intelligence capability, it also relies on cooperation built with foreign partner services in bilateral or multilateral formats at all levels of activity (strategic, analytical and operational). These exchanges constitute an important source of intelligence, contribute to analysis and sometimes allow for collaborative disruption capabilities.

Each service is encouraged to develop relations with its foreign partners in accordance with its remit, and in line with French foreign policy.

3.4. Commitment to security in Europe, NATO and worldwide

At a time when Europe is once again the theatre of a high-intensity war, in an environment of proliferating crises and with the persistent threat of terrorism, interservice coordination is instrumental, in the framework of a joint multilateral strategy.

The active contribution of the intelligence services to the multilateral bodies is key to support the collective defence coordinated by NATO and European strategic autonomy, thereby guaranteeing security in Europe and worldwide. The contribution of intelligence to the interoperability of our forces and systems, with those of our allies, also gives France the means to maintain its international position and help protect our territory and our interests.

Intelligence College in Europe – a French initiative

An example of this collaborative work is found in the Intelligence College in Europe, launched in Paris in 2019 with the support of 31 intelligence communities in Europe. Thanks to their commitment and proactiveness, it provides a series of events every year to bring together the intelligence community, the research community and the policymakers. Celebrating its fifth anniversary in 2024, the Intelligence College in Europe, an intergovernmental initiative independent from the EU, has become a platform for intelligence thinking, sharing and outreach.

For more information: | Pour plus d'informations :

www.intelligence-college-europe.org



Planning and cooperation in the European Union and NATO to tackle the threats

Confronted to threats, France compares and corroborates its analysis with its foreign partners. It stands ready to take action in international coalitions. It is committed thereby in an intelligence-sharing approach with its allies, accordingly with the European Strategic Compass for Security and Defence and the NATO's Strategic Concept.



PILLAR 4:

Intelligence within the rule of
law

4.1. Recognizing the specific features of the public intelligence policy

The sovereign nature of intelligence is such that it exists in a specific framework, “a specialized law” which definition and supervision in France, is the exclusive prerogative of Parliament and Government, with the oversight of constitutional, administrative and ordinary courts. This specific framework guarantees the protection of sources (technical, human and international) and of intelligence officers. In return, these specific features imply the accountability of the services to Government and Parliament.

This duty to account for its action takes the form of strict legal requirements incumbent on the intelligence community: clearance to use intelligence-gathering techniques, hierarchical oversight by state authorities, parliamentary oversight which can be documentary and on-the-spot audits, reports submitted to Parliament and responses to requests for hearings from the Parliamentary Intelligence Delegation. The intelligence services are subject to audits by specialized bodies: French Government Audit Office, independent administrative authorities such as the National Oversight Commission for Intelligence-Gathering Techniques (see below) and the French Data Protection Authority, and the Intelligence Services Inspectorate composed of authorized inspectors from the inspectorates of the ministries with administrative authority upon the intelligence services.

Protection and promotion of the Nation’s fundamental interests – the legal framework for intelligence service action

The French Intelligence Act of 24 July 2015 provides a closed list of the Nation’s fundamental interests legally authorizing the intelligence services to use intelligence-gathering techniques (security interceptions, data acquisition, etc.). Only seven purposes authorize the use of intelligence-gathering techniques, once authorized by the Prime Minister, after a substantiated request from the minister in charge of the service and after an opinion drafted by the independent administrative authority, the National Oversight Commission for Intelligence-Gathering Techniques (CNCTR). These seven purposes are:

- . National independence, territorial integrity and national defence;
- . Major foreign policy interests, implementation by France of its European and international commitments and the prevention of all forms of foreign interference;
- . Major French economic, industrial and scientific interests;
- . Prevention of terrorism;
- . Prevention of attacks on the Republican nature of institutions; actions to reconstitute disbanded groups; collective violence likely to seriously disturb public order;
- . Prevention of organised crime;
- . Prevention of the proliferation of weapons of mass destruction.

4.2. Consolidating the oversight of intelligence-gathering techniques

The French Intelligence Act of 24 July 2015, amended in 2021, established a

legal framework governing the use of intelligence-gathering techniques by the intelligence services, in order to unify scattered legal instruments and to bring existing safeguards up to date. The act provides a closed list of purposes for which the intelligence services are authorized to use intelligence-gathering techniques.

What is the point with protecting secret?

Discretion and secrecy form the prerequisites for the existence of the intelligence services and the effectiveness of their work. Given that the work of the intelligence services consists in gathering strategic information and in disrupting threats, if their working methods were exposed, adversaries would adjust their strategies and behaviours, which would not only endanger our capabilities, but would more importantly, place agents' lives at risk.

As the Constitutional Council put it in 2011, "National defence secrecy is integral to safeguarding the Nation's fundamental interests." The law therefore protects secrecy, subject to strict independent oversight tools. Such is the case with the Commission for National Defence Secrecy (CSDN) and, as far as intelligence is concerned, the National Oversight Commission for Intelligence-Gathering Techniques (CNCTR).

These purposes contribute to the protection and promotion of the Nation's fundamental interests. The act provides for authorization to be issued by the Prime Minister for the use of each intelligence-gathering technique after an opinion delivered by the National Oversight Commission for Intelligence-Gathering Techniques (CNCTR), an independent administrative authority. The act also tasks the Prime Minister with the centralization and traceability of data from the most intrusive intelligence-gathering techniques by the General Secretariat for Defence and National Security (SGDSN) and its relevant operator, the Interdepartmental Surveillance Committee (GIC). This data centralization is key as it guarantees the lawful nature of the techniques used. The CNCTR conducts ex-post audits of this work. New projects will be conducted to update and streamline audits by the CNCTR.

The role of the National Oversight Commission of Intelligence-Gathering Techniques (CNCTR)

In 2015, the CNCTR took over the National Advisory Commission on Security Interceptions (CNCIS). It is an independent administrative authority composed of magistrates and independent experts.

Each surveillance technique is checked prior to clearance for lawfulness and proportionality. Every year, in June, the CNCTR publishes a report in which it presents the outcomes of the use of intelligence-gathering techniques by the services and proposes any relevant courses of action to improve oversight and monitoring of the use of intelligence-gathering techniques.



4.3. Guaranteeing court access

The Act of 24 July 2015 subjects all disputes concerning specifically intelligence-gathering techniques to administrative court scrutiny. Therefore, decisions by intelligence authorities constitute administrative acts that can be disputed.

Cases are adjudicated by a “specialized” panel of the French Supreme Administrative Court which members have security clearance.

4.4. Improving budget steering and performance

Special appropriations, known as “special funds”, are allocated by Parliament to the intelligence services to finance certain targeted expenditure meeting the requirements of confidentiality. They are meticulously audited. Audits are carried out by the Special Funds Audit Committee (CVFS), reporting to the Parliamentary Intelligence Delegation. The services implement the commission’s recommendations to improve their budget management, coordinated by the CNRLT.

4.5. Review of the legislative framework to upgrade the services’ capabilities and level up existing safeguards

A number of changes need to be made to the legal framework. Indeed, the services need new capabilities to respond to evolving threats and technologies and to do so with an eye to balancing the services’ missions with the requirements of the rule of law. These amendments to the legal framework governing the services’ activities will also factor in national and European developments in case law with respect to the safeguards to which our fellow citizens are entitled.

Parliamentary oversight by the Parliamentary Intelligence Delegation (DPR)

The delegation is tasked primarily with assessing the public intelligence policy and with monitoring current affairs and associated challenges.

To this end, the delegation may hear high-level figures including the Prime Minister, relevant ministers, the National Intelligence and Counter-Terrorism Coordinator and intelligence service directors. Its work is covered by national defence secrecy and its members have ex officio clearance to be privy to classified information.

Every year, the DPR publishes a report on its activity, which can contain recommendations and observations for the President of the French Republic and the Prime Minister.

The Special Funds Audit Committee is a DPR body, tasked with auditing the lawfulness of the use, to the last euro, of the special funds allocated to the intelligence services to finance certain targeted expenditure meeting the requirements of confidentiality.

PILLAR 5:

**Harnessing all
the necessary technologies for
intelligence activities**

5.1. Pooling resources for innovation

Technology-enabled intelligence is a key component of the production of intelligence.

The French intelligence community pools a large part of its technological capabilities and develops them primarily in house. This technological pooling is based on four principles:

- Cost optimization for the sound use of public finances;
- Investment rationalization for the benefit of all the services;
- Harmonization of service capabilities for services to have access to the same tools;
- French sovereignty in these areas to limit the country's dependence on foreign technological solutions.

Pooling extends to all technological areas and applies the entire technology-enabled intelligence value chain. New capability developments will comply with the abovementioned principles in all areas from the optimization of data use, such as open-source data, to understanding evolving technologies (artificial intelligence, quantum technology, encryption, etc.). This ambition will be enabled by the development of new interservice networks to cultivate synergies between the members of the national intelligence community.

5.2. Mitigating vulnerabilities – Leveraging opportunities

Confronted with adversaries and threats (terrorist groups and criminal networks in particular) that have made the move to digital tools and states that do not hesitate to make unconstrained use of offensive cyber capabilities and information manipulation, the intelligence services need to constantly anticipate technological developments to adjust their tools and develop new tools.

According to its HR strategy, the intelligence community seeks to recruit the best talents to meet the services' operational needs, leveraging all skills. Experts in data analytics, cryptography, quantum technology, cybersecurity, electronic communications, signal processing and chemistry work together with traditional intelligence stakeholders (analysts, case officers, linguists, etc.).

These close-knit work ecosystems, combining technical and human expertise, are tasked with designing, developing and implementing tools to produce intelligence. They are enabling the existence of committed and operationally efficient work teams.

Complementarity of intelligence sources

The technical data processed by intelligence services represent ever-growing volumes and diversity, calling for the development of tools to detect correlations to be able to convert the data into intelligence.

Within the legal framework, this technical data may be drawn from such sources as interceptions of communications, digital media and satellite imagery.

Technology-enabled intelligence is enriched by human intelligence and vice versa. The French intelligence services are “integrated”, which means that they can leverage in house all the types of sources useful for the production of intelligence.

Growing role of open-source intelligence (OSINT)

An estimated 80% to 90% of information produced in the world is more or less freely accessible. The telecommunications revolution offers huge opportunities for the intelligence community. In addition to the use of social media posts, data from the media, Internet and “grey” literature (government data, academic output, etc.) provide valuable information which, combined with data obtained by other technological and human detection techniques, produce enriched intelligence. The intelligence community has practised OSINT for a long time and is stepping up its collaborative work in this area as it has in the other technical fields.

5.3. Uptaking disruptive technologies

Artificial intelligence and quantum technologies are among the disruptive technologies that will have a major impact on the intelligence services’ activities. They represent threats in that they heighten the potential for disinformation and jeopardize the security of digital communications. However, they also represent opportunities for intelligence.

In these two areas, the intelligence community’s work is based on national strategies called for by the President of the French Republic and actioned by the Government. New collaborative projects will be launched to build up the services’ capacities.

5.4. Fostering national and European tech industries

Thanks to its technical experts, the intelligence community has chosen to insource the majority of its skills for reasons of independence and sovereignty.

This goal will be interfaced with active support for national, and sometimes European, tech industries in the capability areas where strategic independence and resilience in all geopolitical circumstances are instrumental.

Our industrial and technological sovereignty and our autonomous capability to protect the French population, institutions and national territory depends on it.

Artificial intelligence: a source of opportunity clearly identified by the intelligence services

Artificial intelligence (AI) is used daily by the intelligence services to facilitate the work of their analysts. The boom in generative AI, i.e. capable of creating content using its generative model and the data on which it has been trained, offers clear-cut operational opportunities.

However, generative AI also presents a high risk of disinformation, destabilization and proliferation in response to which the intelligence services are organizing, in coordination with the other public administrations, within their remit when it comes to attribute a cyberattack and an information manipulation operation. The intelligence community is supported in this by an excellent French private sector and research community in addition to its own skills.



Countering cyber threats

The intelligence services contribute to anticipate, assess and respond to strategic cyber threats targeting France and its European and international partners, in collaboration with the French National Cybersecurity Agency (ANSSI), a General Secretariat for Defence and National Security body responsible for coordinating government cyber defence. The intelligence services and the ANSSI support the judicial authorities and services in their work to counter cybercrime.

PILLAR 6:

Attracting and
promoting skills in the
French intelligence
community

61. Engaging with strong, distinctive professional values

The work environment in the intelligence services is geared to very high standards where discretion, loyalty and a sense of service go hand in hand with team spirit, initiative and professional commitment to assignments contributing directly to the public interest.

To protect France and French nationals, intelligence community agents conduct vital work with rigour and dedication, using information from a wide range of sources to inform government decisions and anticipate, act on and disrupt threats. This commitment is quite a meaningful feature in a professional career.

Despite their particular working methods, the intelligence services make every effort to stay connected with society and to include our fellow citizens' aspirations in their human resources policies such as actioning innovative, meaningful working methods supportive of high-quality service and environmental protection.

62. Attracting talents to a community rich in its diversity of jobs

With 250 different jobs, the intelligence community demonstrates huge professional diversity and vitality. The community's agents work on intelligence from human, digital, technological and financial sources, as linguists (often in rare languages) and in key support functions. Men and women of this community fulfil sensitive and varied missions in stimulating environments with opportunities to strengthen their skills thanks to in-service training and to the Intelligence Academy.

A solid training mechanism based on in-service training and Intelligence Academy courses

Working in the intelligence community opens the door to a multitude of internal and external career prospects in different geographic areas, fields and intelligence services, with varied and growing responsibilities and even in new occupations. Each service provides onboarding pathways and basic and continuing training for agents to adjust to the challenges and variety of their assignments.

Intelligence community agents also benefit from training courses and outreach days organized by the Intelligence Academy (ACADRE), which was created in 2010 and is run under the authority of the CNRLT. The Intelligence Academy thereby contributes to fostering closer ties between the services as an exclusive platform for discussions and information-sharing in association with the academic and research communities.

63. Retaining talent by building rewarding career paths

The different human resources departments conduct an ambitious policy to recruit the best talents by means of pay packages, rewarding career paths for the diversity of skills and profiles, constant enrichment of experiences and continuous upskilling by active, world-class, state approved training courses.

This professional development cultivates the strengthening of expertise and personal qualities, with benefit within the intelligence community and beyond.

The intelligence community has developed an employer brand

To embody our human resources policy, the intelligence community has developed an “employer” brand that reflects the purpose of intelligence: prevent breaches of national security, protect people, goods and institutions, and protect and promote French interests. This “employer” brand is a commitment from the intelligence community to raise our profile, build our appeal and communicate our professional opportunities for every individual to feel as a fully-fledged part of our community.

64. Making mobility a driver for attractiveness and unity

In addition to rewarding careers in one specific service, the ten services of the intelligence community encourage and promote mobility to discover other positions and administrative cultures and acquire new skills. The ambition is to cultivate mobility in both the intelligence services and in other environments where agents can continue to have a feeling of fulfilment: other key French government departments (security, foreign affairs and defence), European institutions, the Defence Technological and Industrial Base (DTIB) and, more generally, any activity sectors.

65. Building ambitious, appropriate and inclusive human resources strategies and policies

HR policies take the form of assertive processes to promote equality and diversity. The actioning of innovative measures, simultaneously with the developments in the civil service, consequently enables the services to respond with efficiency and agility to evolving threats, technological change and a multitude of operational constraints.

These policies are sustained by a significant and unprecedented increase in human resources granted by the Nation for its domestic protection and abroad.

The Directorate General for the Administration and the Civil Service and the relevant ministries’ human resources departments are all actively engaged in continuing to develop the intelligence services’ human resources.

“To serve France and protect the French people, you contribute quietly to extraordinary assignments, serving the State authorities.”

Keen to take up the challenges of French intelligence? Join our community!

<https://choisirleservicepublic.gouv.fr/metiers/nouvelle-maquette-renseignement/>

