

## CHAPTER 8

# KNOWLEDGE AND ANTICIPATION

In an international environment marked by great uncertainties and potentially extremely short warning periods, a country's first line of defence are its capabilities for knowledge and anticipation. These must offer decision makers, as much prior to the crises as possible, the necessary basis for assessing the situation (the variety and gravity of risks and threats, opportunities for French and European interests, etc), enabling them to make better-informed choices between the different possible modes of action. Consequently, the knowledge and anticipation function has been elevated for the first time to the status of a strategic function in its own right and embraces several areas.

### *Intelligence*

The purpose of intelligence is to enable the highest authorities of the State, together with our diplomacy, armed forces and our internal and civil security services, to anticipate developments, and to reach assessments, decide and act in full independence.

By presenting the state of risks, threats and opportunities in the widest spectrum of fields (political, military, economic, energy, etc.) as comprehensively and accurately as possible, intelligence serves to enlighten decisions, as well as to foreshadow, support and review action.

It must therefore maintain a permanent vigil to detect new risks and the first signs of developments affecting our security. It provides a basis for the planning and conduct of operations. It must give France the capacity to preserve the strategic initiative and retain its ability to decide independently.

The acquisition of intelligence flows from several different groups of activities working in close association, namely: information gathering in the field, through human or technical sources; the work of civil and military intelligence services; and the activity of specialised military units. In all cases, the information is exploited, cross-checked, synthesised and analysed, before being transmitted to decision makers.

This presupposes on the one hand an organisation designed to promote the dissemination and assimilation of information in real time, and on the other the upgrading of our information-gathering and processing capabilities.

*The systematic enhancement of our intelligence means will be the object of an overall planning process to be implemented according to four main priorities*

## AN INDISPENSABLE FOCUS ON HUMAN RESOURCES

Intelligence depends in the first place on the people who gather, analyse and exploit it, sometimes in dangerous conditions. The greatest attention will therefore be paid to the recruitment, training and careers of intelligence personnel. Human resources management will be overseen jointly by the relevant ministries and services in order to optimise this function (chapter 14).

### Recruitment and career management

Staffing levels will be reinforced and recruitment will be stepped up, notably as regards the fight against terrorism, counter-proliferation, fighting organised crime, combating espionage and economic interference. The number of technical personnel such as engineers, technicians, linguists, imagery interpreters and specialists in the programming of these capabilities will also be increased.

Particular emphasis will be placed on creating enhanced career tracks in intelligence. Recruitment needs to be not only limited to the specialised and technical civil service channel, but also open to the universities and *grandes écoles*, with easier recourse to personnel under contract.

Common careers management norms will be laid down regarding the recruitment and mobility of personnel, as well as initial and continuous training. An intelligence academy will formulate a training programme serving as a fully-fledged “core course” to be developed among the different intelligence services, run by them and sanctioned by a diploma recognised by them all.

Human resources should also be better used, for example, with regard to rare languages. Encouragement should be given to cross-postings by secondment between the different services, as well as to greater mobility between services and ministries.

## Human intelligence sources

Special emphasis will be placed on human sources of intelligence, as part of the overall effort. This implies efforts in terms of manpower, quality of recruitment, training of the personnel in charge of this mission, as well as an increase in the recruitment of sources and an improvement in their geographical distribution according to the newly defined priorities.

## DEVELOPING TECHNICAL CAPABILITIES

The rapid pace of technological change calls for expanded technical means to better ensure the security of the country. A qualitative and quantitative leap is particularly necessary for France to remain at a level enabling it to dialogue with the handful of countries that are its major interlocutors, both present and future, in the intelligence sphere. These countries have sharply enhanced their capabilities since 2001, while the French services have not done so to the same degree.

The performance of intelligence services and military units will be enhanced in order to respond to the growing needs resulting from our new strategy. In certain areas it is essential to guarantee the complementary fit between the various sources—space-based, land-based, sea-based and airborne. A qualitative and quantitative effort will be initiated, *starting in 2008*, and will be pursued continuously over the next 15 years.

The Internet has become crucial to our security. The Government's technical capabilities in this sphere will be strengthened, with a greater number of specialised technicians and experts placed at its disposal.

The effort will also concern activities in space, a key factor of strategic independence. Space-based assets, freed from the constraints bearing on aerial overflight, can cover a broad array of needs from strategic vigilance to the planning and conduct of operations.

*Imagery intelligence* (IMINT) is based on complementary resources at the strategic level (observation satellites), operative level (*i.e.*, on a theatre of operations) or at the tactical level (*i.e.*, on the ground, using human observers, drones and airborne sensors). Space imagery requirements are currently covered by the Helios 2 programme for

### **Space intelligence and the fight against proliferation**

The fight against proliferation, and particularly ballistic proliferation, illustrates the potential contribution of space-based intelligence as a complement to other sources, human in particular. The earlier the intelligence arrives here, the better it can help to prevent risks and plan responses.

The highest State authorities must be in possession of the maximum amount of information from national sources regarding the origin, the credibility of the threat and the intentions of potential adversaries. This implies reinforcing our capacities in the field of observation satellites (visible spectrum, infrared and radar) and constituting the means of detection and early warning (radar and space-based) of ballistic missile launches (see the protection function, Chapter 11).

very high resolution images in the visible spectrum and infrared images, and by the addition of all-weather imagery provided by exchanges with Germany and Italy, thanks to the SAR-Lupe (2007) space systems in the former case, and to the Cosmo-Skymed (2009) programme in the latter. A *European programme*, MUSIS (multiuser satellite imagery system) is expected to permit the launch of the next generation of space sensors. The visible spectrum component will be reinforced in 2015 *via* a reconnaissance asset providing ultra-high resolution images, together with superior identification capacity. At the same time, Germany and Italy plan to develop their radar capacities. To avoid the risk of discontinuity at the end of the life of Helios 2B, France will begin work on the visible spectrum component of the MUSIS programme as from 2008.

As regards airborne capabilities, the effort will focus in particular on drones, remotely piloted air vehicles providing control over information in crisis theatres and thereby facilitating the operational engagement of our forces. A MALE (medium altitude and long endurance) UAV system is expected to be operational in the middle of the next decade. This will carry a more comprehensive intelligence gathering capability than what is currently available with tactical drones.

The effort will also focus on new generation on-board systems carried by combat aircraft.

*Signal intelligence* (SIGINT) embraces the gathering, positioning, identification and interpretation of electronic signals. This helps to enhance our independent capacity to assess situations and improve our forces' capacity to protect themselves. The space component will be covered by the CERES (space signal intelligence capability) programme,

which is open to European co-operation, to be launched in the short to medium term in order to be operational by the middle of the next decade. In the airborne sector, the effort will notably concern on-board sensors equipping the successors to the Transall *Gabriel* aircraft, and a UAV capability. It will also include land-based means including advanced transmissions detachments, and seaborne assets in the form of an “acoustic intelligence” ship and nuclear attack submarines.

Overall, the share of annual intelligence service budgets earmarked for technical investment will therefore need to be increased.

To signal the priority given to all joint assets contributing to knowledge and anticipation, the Defence General Staff will develop a *specific planning and programming process* for this sector.

## THE NATIONAL INTELLIGENCE COUNCIL

The existing perimeter of the intelligence services reflects the diversity of their missions. There is therefore no plan to modify these beyond the recent reforms, which have enhanced the effectiveness of the setup and which led to the creation in 2008 of the *direction centrale du renseignement intérieur* (DCRI Central Directorate for Domestic Intelligence).

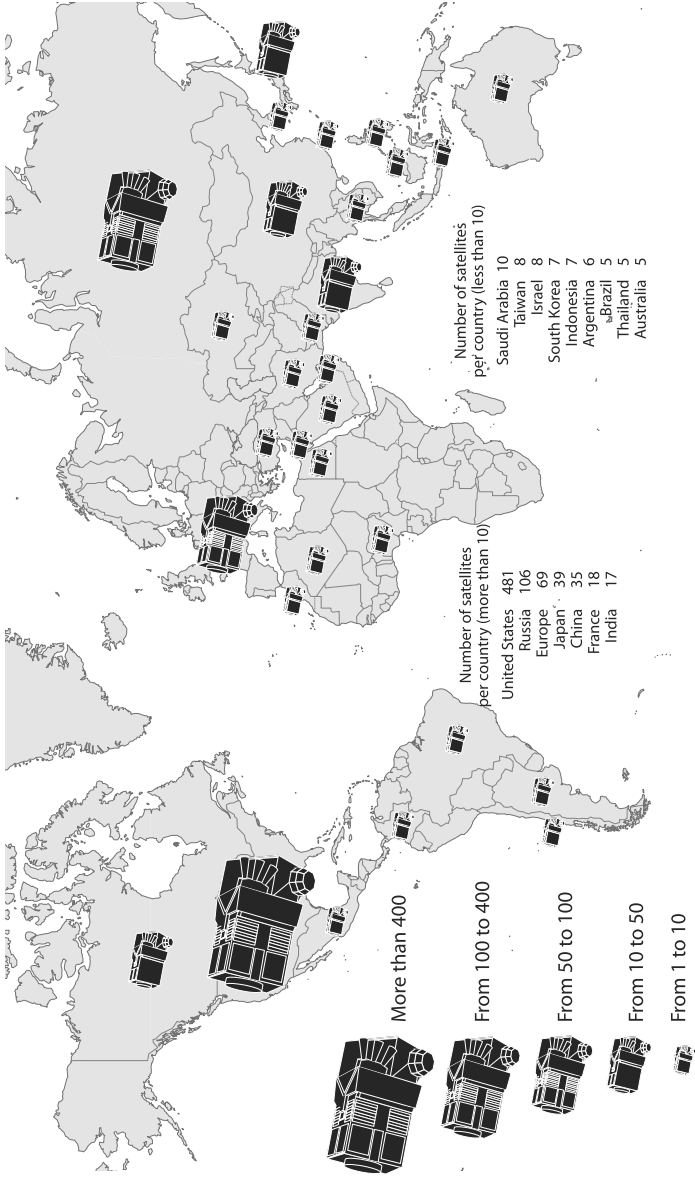
However, the intelligence organisation needs to be better coordinated, with a more clearly defined complementary fit than is currently the case.

The governance of the intelligence organisation will therefore be reinforced with the setting up of a National Intelligence Council.

At the operational level, already existing co-operation between the services of a single ministry or different ministries will be formalised and stepped up in new areas. The aim is to avoid dispersal of effort and human resources within a tight budgetary context, and making better use of resources, developing synergies between services with common aims, and avoiding duplication or gaps in coverage. Within the framework of these forms of co-operation, policy with regard to equipment should give rise to systematic pooling. The bulk of the technical assets and investments is concentrated in the Ministry of Defence, with the means at the disposal of the *direction générale de la sécurité extérieure* (DGSE) and the *direction du renseignement militaire* (DRM).

In the fight against terrorism, the *Unité de coordination de lutte contre le terrorisme* (UCLAT Anti-Terrorism Co-ordination Unit), which reports to the Director General of the National Police, will continue to co-ordinate the competent services.

Main satellite-owning countries



Source: Ministry of Defence (open sources).

### The French intelligence services

French intelligence is organised around a series of complementary services, namely:

Two general-purpose services: the *Direction générale de la sécurité extérieure* (DGSE General Directorate for External Security), which is responsible for the gathering and analysis of intelligence outside the national territory, and the *Direction centrale du renseignement intérieur* (DCRI Central Directorate for Domestic Intelligence), the intelligence and police investigation activity of which is focused on the national territory;

Four specialised services: two services supporting the ministry of Defence and the Armed Forces—the *Direction du renseignement militaire* (DRM Directorate for Military Intelligence) and the *Direction de la protection et de la sécurité de la défense* (DPSD Directorate for Defence Protection and Security); and two services specialised in customs and financial questions—the *Direction nationale du renseignement et des enquêtes douanières* (DNRED National Directorate for Customs Intelligence and Investigations) and the *Traitement du renseignement et action contre les circuits financiers clandestins* (TRACFIN—Intelligence Processing and Action Against Illicit Financial Circuits).

Altogether, some 12,000 men and women work directly for the intelligence services. In addition, the Army, Navy and Air Force have specialised military units performing military intelligence missions; these employ 4,000 people.

Intelligence regarding the economic sphere is the domain of the general-purpose intelligence services as well as those services more specialised in this sector (*i.e.* DNRED and TRACFIN). Their activity needs to be distinguished from what is known as “economic intelligence”, which is based solely on the analysis of information from openly available sources.

At the strategic level, a new echelon of co-ordination between intelligence services will be put in place. It will set policies, apportion objectives and arbitrate between competing requirements. The new setup will be articulated around a National Intelligence Council and a National Intelligence Co-ordinator working in the Office of the President of the French Republic.

Plenary meetings of the National Intelligence Council will be chaired by the President of the French Republic and will be attended by the Prime minister, the Ministers of the Interior, Defence, Foreign Affairs, Economy and Budget, and where appropriate by other ministers depending on the agenda. The National Intelligence Co-ordinator

and the heads of the relevant services will also attend, as well as the Secretary General for Defence and National Security<sup>1</sup> who will act as secretary to the Council.

The Council will set the broad strategies and priorities for the intelligence services. It will approve a planned timetable for objectives and human and technical resources, provide guidance and arbitrate with respect to the legal framework of intelligence services activities. It will meet at the request of the President of the French Republic, in a more limited format, to be known as the Restricted Council for Intelligence.

A National Intelligence Co-ordinator will be appointed, reporting to the Secretary-General of the Office of the President, with a small support staff. With the assistance of the General Secretariat for Defence and National Security, he will prepare the decisions of the National Intelligence Council and follow through their implementation. He will oversee the planning of intelligence objectives and means, notably *via* the annual investment plan, and will oversee its execution. He will chair the inter-ministerial technical investment steering committees on intelligence matters.

He will be the conduit for the intelligence services to the President of the Republic.

He will chair the periodic meetings of the directors of the intelligence services in order to establish intelligence research priorities and examine intelligence services' requests. The Prime minister's office will take part in these meetings. This new organisation is also expected to improve the flow of the most relevant intelligence.

The General Secretariat for Defence and National Security will support the work of the National Intelligence Co-ordinator and will organise task forces on subjects selected in the light of priorities set by the National Intelligence Council.

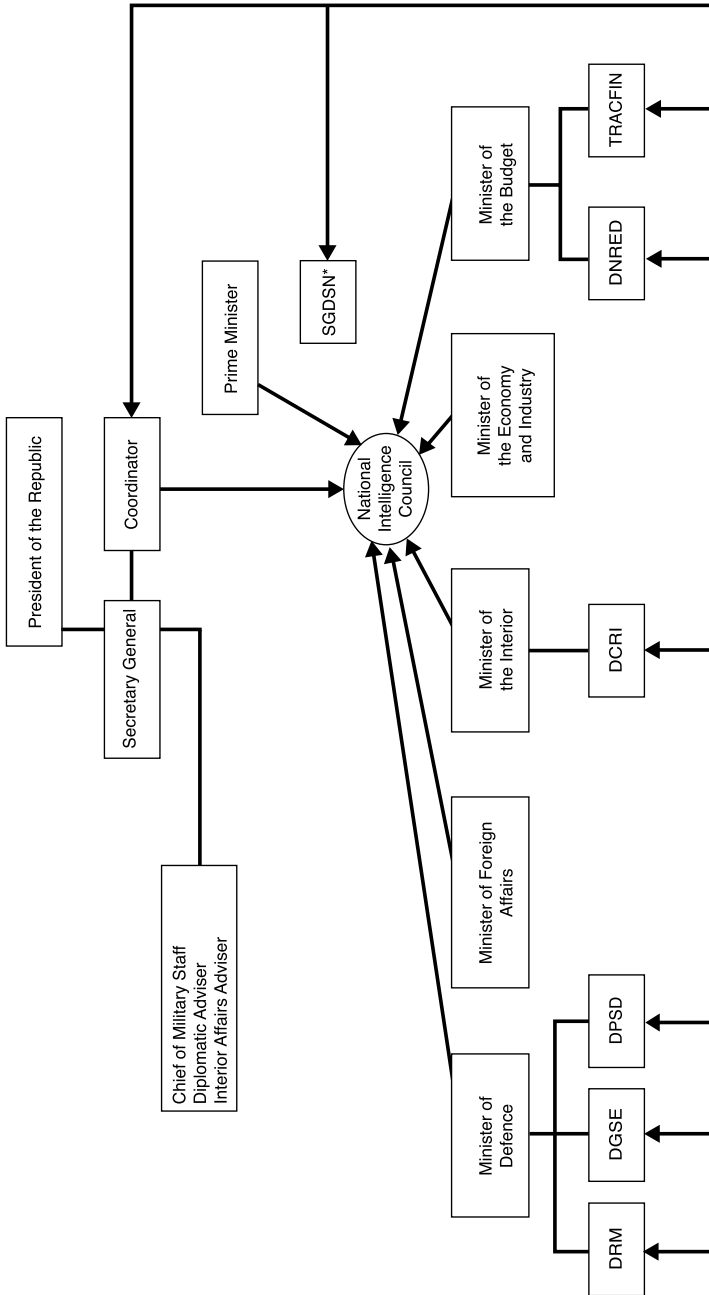
At the same time, the information on the activity of the intelligence services will be guaranteed by the Joint Parliamentary Delegation for Intelligence (*délégation parlementaire au renseignement*). These activities will be subject to external control by the competent independent administrative authorities, and in particular the National Commission for the Control of Security Intercepts (*commission nationale de contrôle des interceptions de sécurité*), and the Commission for the Verification of Special Funds (*commission de vérification des fonds spéciaux*).

---

1. Which will replace the Secretariat General for National Defence.



The new organisation for intelligence



\*Secretariat of the National Intelligence Council and the permanent inter-agency committees

## AN APPROPRIATE LEGAL FRAMEWORK

Intelligence activities currently lack a clear and adequate legal framework. This shortcoming needs to be remedied. Consequently, the new legal framework will define the missions of the intelligence services, together with the guarantees given to personnel and human sources, along with the principal arrangements for the protection of national defence secrets. Legislation will be adapted, respecting the balance between the protection of public freedoms, effective prosecution before the courts, and the safeguarding of secrecy.

For this purpose, a legislative definition of the intelligence services' missions will be formulated, covering all of their missions. It will be sufficiently precise for the needs of personnel of the intelligence services concerned. Similarly, provisions will be enacted to protect the anonymity of intelligence personnel, regulate the conditions under which they may resort to covert identities and punish the disclosure or revelation of the identity of an agent or his/her membership of the intelligence services. Similarly, the disclosure of the identity of agents will be protected in the course of administrative or judicial proceedings, and provision will be made for the protection of the intelligence services' sources and external agents: the divulgence of information liable to reveal their identity will also be prohibited and punished.

The protection of national defence secrets needs to be adapted and strengthened. In accordance with an opinion of the French Council of State (*Conseil d'Etat*)<sup>1</sup> issued on April 5, 2007, the definition of national defence secrets and their disclosure will include classified information, classified networks and certain highly sensitive locations the existence or purpose of which in and of itself is a national defence secret. Specific rules for judicial searches conducted in classified locations or in locations containing national defence secrets will also be enacted by law.

There is a need for broader powers of consultation of technical data and administrative databases referred to in the January 23, 2006 Act on the fight against terrorism, or that of investigative police files. In addition, exchanges of information between DNRED and TRACFIN on the one hand, and the other intelligence services on the other, will be authorised by law. At the same time, the July 10, 1991 Act on electronic communications secrecy will be adapted to take account of recent technical developments.

Altogether, this amounts to an all-embracing, systematic, long-term approach to our national intelligence system to enable it to answer the need for the future protection of the interests of the nation.

---

1. The Council of State is the French Administrative Supreme Court.

### **The role of space in the national defence and security strategy**

Outer space has become as vital to global economic activity and international security as the sea, the air or land environments. Like all of its European Union partners, France is opposed to turning space into a new battlefield. Our country has no plan to place weapons in space and will continue its diplomatic efforts in favour of the non-militarisation of space.

On the other hand, the deployment in space of all types of satellites—communications, observation, listening, early warning, navigation, meteorology, etc.—has become an indispensable element for all strategic functions. Consequently, our country will make a special effort in the area of space to ensure its coherence with the needs of our defence and national security.

**This ambition in space will concern simultaneously:**

— *Capabilities*: the country will ensure the continuity and modernisation of its observation and communications satellites which have now become indispensable to intelligence gathering on the one hand, and to the conduct of military interventions on the other: the visible spectrum segment of the MUSIS programme will be launched starting in 2008 with a view to be operational in 2015.

France will establish a significant SIGINT satellite capability in the wake of the success of experimental satellites in this area: the CERES satellite system will be completed in the middle of the next decade. To counter the ballistic missile threat, a missile-launch detection and early-warning capability will be put in place between now and 2020, preceded by the deployment of a pilot system in the course of the next decade. Space situational awareness, which now has major civil and military implications, will be the subject of a particular effort in conjunction with our European partners.

In general, European co-operation in space will be encouraged, notably by the pooling of assets.

— *Budget*: average annual funding for space programmes, after falling to EUR 380 million in 2008, will be doubled over the coming period.

— *Organisation*: in view of the growing importance of space for defence and national security, doctrine, operations and programmes in the field of space will be placed under the responsibility of an identified, dedicated joint command, under the authority of the Chief of Defence Staff. Under this new command, the Air Force will be given increased competence in the management of space assets.

## *Knowledge of potential theatres of operation*

Knowledge of potential theatres of operation is a key precondition of all forms of military action. Due to its geography and its international responsibilities, France is particularly attentive to this dimension. The French overseas *départements* and territories cover a total surface area of 122,000 sq. km, spread across the globe. This presence puts France in a favourable position in terms of its knowledge of sensitive areas of the world.

### FRANCE'S PRESENCE IN THEATRES OF OPERATION

Knowledge of potential theatres of operation comes from regular familiarisation with the areas concerned. The first priority in this regard is the strategic axis stretching from the Atlantic to the Indian Ocean, notably through information-gathering by all of the technical sensors (space-based, airborne, onshore and naval) to which our forces have access. Our knowledge will also benefit from our pre-positioned assets in Africa and the Gulf, and from our forces in the French Caribbean and French Guyana, the Indian Ocean and the Pacific.

### AREA STUDIES

We also need insight into the politics, society and cultures of potential theatres of operations. Here, greater use should be encouraged of the work performed by research centres, think tanks and institutes, as well as that of universities with specialists in existing and potential hotspots. The State's own prospective and policy-planning centres will commission studies on these regions.

### GEOPHYSICAL DATA REQUIREMENTS

Developments in weapons technology, the greater complexity of actions to be carried out, and the need to minimise collateral damage put data concerning the geophysical environment at the heart of the management of defence systems. Ten years ago, very few weapons systems used such data. Today, no weapons system is unaffected by this capacity.

Knowledge of potential theatres of operations therefore also requires the acquisition of these data, which depend notably on mapping and meteorology.

Programmes exist for gathering these kinds of data, including digital geographic data, hydrographical and oceanographic data, and meteorological data. An overarching approach at the national and European level will be undertaken to structure the global data gathering capability and the utilisation of these data in weapons systems. Efforts will focus in particular on developing responsiveness in order to facilitate rapid deployments. This capability is particularly important in view of the fact that France may have to assume command responsibilities for operations in these areas.

### *Benefiting from the diplomatic network*

Thanks to its bilateral embassies, multilateral representations and consular posts, our country boasts an exceptional external information network and window onto the world. This network plays a prime role in the gathering, circulation, sharing and analysis of information, for the most part from open sources of all kinds, by all of the different Government services present abroad.

Efforts will be made to ensure that those in charge of our diplomacy are better able to exploit openly available information, analyses of diplomatic sources and intelligence provided by the specialised services. This implies expanding exchanges among the different Government services working in the countries concerned, under the authority of the French ambassadors, and cross-checking the different sources.

These exchanges should be made systematic and could take practical shape, for example, in the form of regular meetings of a restricted committee in each embassy in the presence of the ambassador.

At the level of the central government administrations, all of the information gathered in the field needs to be compiled and collated. Working relations between the Ministry of Foreign and European Affairs, the other ministries and specialised services will be intensified. The aim is to achieve common and multidisciplinary analyses of security risks

## “Horizon-scanning”

There is a need to develop a “horizon-scanning” approach by the Government, in universities and in defence and security circles, in order to anticipate emerging risks and threats, opportunities for French and European interests, and to guide preventive policies and assets in a timely fashion.

This approach should permit greater comparison between analyses. The areas concerned are multi-disciplinary and inter-disciplinary, covering military and security strategy, geopolitics, human sciences, economics, and scientific and technological research.

The resulting needs call for:

— Co-ordination of efforts within the Government and by setting up an inter-ministerial network consisting notably of the General Secretariat for Defence and National Security, the Ministry of Interior (Delegation for Prospective and Strategy), the Ministry of Defence (Directorate for strategic affairs), the ministry of Foreign and European Affairs (Policy Planning Staff), and the *Secrétariat d’État* for Prospective, Public Policy Evaluation, and Development of the Digital Economy (Centre for Strategic Analysis):

— Setting up a common Internet portal for this purpose to present a comprehensive view of the competencies of the different prospective centres; research themes and intellectual output will be made more widely known, with systematic calls for projects;

— Encouraging synergies and instituting links (fora for exchanges of views, etc.), and even pooling or networking of facilities (vigilance units, documentation centres, etc.), between government departments and academic circles, research centres, private institutes, think-tanks and industry;

— *Support for research on defence and security, via* a financial effort aimed at developing and maintaining competencies available for mobilisation by Government. University research centres and other research institutes and think tanks are seriously under-funded at present if we compare with our main partners. This spending will be stepped up in the short and medium-term. This will be accompanied by rationalisation of the commissioning of work at the inter-ministerial level in order to be able to respond to Government requirements in a timely fashion, and improved circulation of information within administrations;

— The development of international exchanges, especially within Europe, working through our diplomatic network and the European external action department currently being set up. Also, a particular effort will be made towards the European framework programme for research and development.

## *Knowledge management*

The notion of “knowledge management” spans the capacity for civil and military decision makers as well as State personnel in the field to gain access in a timely fashion to information and to make optimal operational use of it. The aim, in normal circumstances as well as in time of crisis, is to ensure that all National Security actors are able to share the relevant information and that decision makers are in a position to formulate and transmit the necessary orders at the right time.

The four pillars of knowledge management are:

— The timely transmission of information between decision-making centres and places of execution thanks to adequate dataflow capacity;

— Interoperability between information networks, to optimise the flow of information;

— Protection of information (information systems security), ensuring the confidentiality, availability and integrity of the system and the information processed;

— Verification of information, ensuring that it is reliable, flows smoothly and is properly utilised.

Secure, reliable, real-time access to information is an essential condition of sovereignty and freedom of action. This is indispensable to the capacity to be first on the scene in a theatre of operation and to guarantee the capacity to intervene as a framework nation.

Knowledge management will apply at the strategic level, *i.e.*, at the level of the top civil and military decision makers, as well as at the operational and tactical levels.

At the strategic level, the aim is to network all of the officials concerned in order to optimise the decision-making process. This implies extending the ISIS (secure inter-ministerial intranet) inter-ministerial network, and guaranteeing by means of an appropriate space-based communications system covering the entire planet, permanent interaction between the governmental decision-making centres and our forces deployed on the battlefield.

At the level of operations, the priority is to deploy tactical radio capabilities, to equip our forces with broadband networks and develop the digitalisation of the operational space. The aim here is to optimise our knowledge of situations in the field and the use of weapons systems engaged, and to integrate each level into a coherent overarching architecture, linking governmental situation centres to commanders in the field.

In all instances, the need is for secure interoperable communication networks (intra-and inter-ministerial) on the one hand, and on the other effective information sharing and processing systems (computer assisted decision-making, information display, secure messaging, etc.), thereby reducing the time required for processing and strengthening networking. These networks should also permit exchanges with our main partners and allies.

Current and future developments relating to information systems will radically transform decision-making processes, giving rise to new practices in the exercise of decision-making at all levels, as well as in the conduct of military and security actions. Consequently, alongside the requisite effort where equipment is concerned, greater emphasis will also be placed on training, adaptation and organisation.



### **Key decisions relating to knowledge and anticipation**

- **Organisation and coordination**

- Creation of a National Intelligence Council under the authority of the President of the French Republic;
- Appointment of a National Intelligence Co-ordinator in the Office of the President of the French Republic;
- Drafting legislation on intelligence services activities including provisions for the protection of national defence secrets and the protection of personnel;
- Improving the diplomatic network to ensure better sharing of information, mostly from open sources, among all State services abroad; building awareness of intelligence issues in the diplomatic network;
- Co-ordination and development of a prospective approach within Government, in particular by setting up an inter-ministerial network.

- **Human resources and training**

- Upgrading of intelligence career tracks; creation of an intelligence academy;
- Recruitment of specialists (engineers, computer specialists, image interpreters and linguists, in particular) in order to upgrade technical capabilities and competencies, together with cross-specialty experts;
- Greater efforts in the field of knowledge of potential theatres of operation, in particular by promoting understanding by Government personnel of the cultures of foreign countries.

- **Technical investments**

- Strengthening the technical capabilities of the intelligence services in response to the development of information and communications technologies, notably the Internet;
- A new approach to the planning of space-based intelligence, with a major emphasis on imagery and signals intelligence;
- Enhanced airborne imagery and signals intelligence gathering capabilities, with particular emphasis on drones;
- Development of geophysical data-gathering capabilities and application by weapons systems;
- Developing knowledge management capabilities in order to optimise decision-making, and digitalisation of the operational space.

