CHAPTER 11

PROTECTION

In the light of the new emphasis on protection of the population and territory, France will need the capability to meet four main priorities.

In the new security environment, the first of these priorities will be to ensure *the permanent mission of protecting* the population and territory, particularly through in-depth surveillance and control of national territory and its approaches.

The French resource strategy will need to incorporate *the objective of overall resilience as a key objective* (see Chapter 3) for society and the authorities, in order to ensure at all times the continued functioning of the authorities and the continuity of national life.

In addition, steps must be taken to overcome the failings and gaps in the French capability to respond to *new and unconventional forms of threats and vulnerabilities*.

Finally, France will need to develop the *rapid reaction capability of its authorities* in the event of a major threat arising on national territory and if the national protection posture needs to be raised in response to an external threat. This calls for a new approach to the management and co-ordination of civil and military capabilities.

The fight against terrorism

The Government *White Paper* on domestic security against terrorism, published in 2006, has already highlighted the need for changes to France's anti-terrorism system. This depends in the first place on the work of the national police (UCLAT Anti-Terrorism Co-ordination Unit), the intelligence services and, when needed, outside France, specialised units of the armed forces.

Protecting the population and the integrity of the nation against terrorist threat implies:

Forestalling the risk by surveillance, detection and neutralisation of dangerous movements of persons and goods, and protecting national territory from incursions;

Protecting particularly vulnerable targets, such as air, land and maritime transport networks, critical infrastructure and critical information systems;

Staying one step ahead of the evolving threat situation by developing technological superiority in the fields of CRBN protection, explosives detection, control of telecommunications traffic, video-surveillance, information systems protection and biometrics.

The government's "Vigipirate" plan establishes a clear set of operational vigilance, prevention and protection measures that can be adapted to the threat assessment.

Protecting the nation against crises on a wider scale

In-depth control and surveillance of national land, sea and air space

Control and surveillance of national land, sea and air space must adapt to the massive increase in exchanges and communications brought about by globalisation. In due course, a European *security strategy will be need to be formally agreed*, covering the *maritime, air and space sectors*. The strategy will help to co-ordinate the work of the European Union, civil agencies and the European Defence Agency.

Movements of persons and goods

Security measures have traditionally focused on the physical protection of facilities, but must now *turn more towards prevention and focus on movements* of persons *and flows* of goods. This capability is currently severely limited by legal, technological and economic constraints.

France will propose the adoption by the EU of legislation requiring transport companies to provide advance information on goods exported to European Union territory. This approach will make it possible to carry out risk assessments and, if necessary, to issue a ban on exports of goods to France or apply stricter control measures on arrival.

As far as controlling the flow of persons is concerned, France will support the European Commission's initiative to work towards the long-term development of a system for controlling movements at the external borders of the Schengen zone through the introduction of a system of recording entries and exits.

Automated control systems will be developed to support this initiative (biometric recognition and the associated databases).

While respecting individual freedoms, improvements will also be made to the use of databases on travellers using public transport, particularly by air and sea, compiled by operators as part of their commercial activities.

As regards controls on the flows of goods, France will contribute to enhancing the security of international supply chains by supporting the development of merchandise identification and monitoring systems and content detection systems of illicit or dangerous materials. Applied research backed up by parallel experiments in conjunction with industry will be carried out in order to propose attainable standards and reliable equipment to carry out such controls without reducing the smooth flow of goods.

Protecting our maritime approaches

Maritime surveillance and intervention assets must be designed not only to make a more effective contribution to the fight against terrorism but also to carry out all the missions *incumbent on the State at sea* (protecting national interests, safeguarding of persons and goods, combating illicit maritime activities, protecting the maritime environment and resources, etc). These assets include the semaphore chain, surveillance vessels and aircraft and helicopters. They are intended to operate in waters where France has not only sovereign rights but also duties (territorial waters, exclusive economic zone, international

waters in accordance with the provisions of international conventions). *Most of these assets will need replacing over the next fifteen years*. Optimisation will be pursued, with the aim of acquiring *units that are relatively unsophisticated but capable of operating on the high seas*. This requirement is essential to guarantee Navy missions in this field, and to draw a clear distinction between the assets it requires for these tasks and those destined for military engagement and combat missions, such as first-rank frigates, for example.

Land-based surveillance assets will be reinforced, pursuing deployment of the integrated inter-ministerial national surveillance network, which will be linked to other European maritime surveillance systems. Efforts will continue to improve the protection of key strategic civil and military ports, in particular their harbours, in line with maritime and port security doctrine. The funding required for the acquisition of these resources will be allocated in light of the inter-ministerial nature of maritime protection.

At the European level, France will propose plans to introduce new capabilities such as *maritime surveillance drones, automatic station-keeping satellites, trans-horizon radar, integrated maritime intelligence systems, etc*.

Air surveillance

France's air detection network will be modernised to strengthen our capability to defend against any air intrusion by detecting the threat before it enters French airspace. Over the short and medium term, the oldest air defence radars will be replaced; more recent equipment will be upgraded and new low-altitude radars will be deployed to improve national coverage and lower the radar floor. Detection ranges will be extended, most notably in the Mediterranean, thanks to the acquisition of *trans-horizon radars*. Over the longer term, efforts will be made to develop resources capable of detecting and intercepting most small, low-speed aircraft in French airspace.

Outer space

Military and civil activities depend increasingly on space-based assets performing vital missions and services. This situation creates a new vulnerability, as the amount of space debris in orbit grows and direct attack capability appears to be within the reach of a number of national powers.

Constant detailed tracking of objects orbiting the earth is now the sole preserve of the United States and, to a lesser extent, Russia. *Europe is dependent on other powers for the surveillance of outer space.*

In order to overcome this dependency, avoid foreseeable collisions and forestall hostile acts, France will encourage the development of *a European project to detect and monitor objects likely to cause damage to missile launchers or satellites*. In the short term, the project will form part of GRAVES, the French space surveillance system currently operational at the *national* level only. In the longer term, this capability will form part of a more global strategy for the protection of our space-based infrastructure.

RESPONSE TO THE EVOLVING THREAT SITUATION

Reinforced protection against CRBN threats

In response to the scale of the challenges posed in a field which is both complex and costly, France will substantially upgrade its response and improve co-ordination between the various authorities. This process will be steered by a strategic committee tasked with ensuring the overall consistency of capabilities designed to protect against these threats and the proper execution of research and deployment programmes.

One of the first priorities will be to support and strengthen the national network of Biotox-Piratox laboratories set up in 1997, following the sarin gas attack on the Tokyo subway, to identify and characterise the most dangerous agents.

In this domain more than in any other, *joint training programmes and exercises will be developed* in order to simulate the conditions of such an attack as realistically as possible for all those potentially involved—emergency, security and medical services—and hone joint intervention procedures.

The Defence and Interior ministries will set up *a joint national civil and military training centre*. Equipment and training of civil and military units will be boosted with the emphasis on shared identification of threats. *All first-line response personnel in the public security apparatus will gradually be equipped with appropriate CRBN protective gear.*

The resources allocated to the defence zones—renamed defence and security zones (see box)—will need to be stepped up and include, to a far greater extent than is currently the case, mobile facilities for the detection, sampling and identification of biological and chemical agents. Decontamination facilities will be expanded, in the short term to three times the number of decontamination chains currently deployed nationwide. Some of the powers currently reserved exclusively to the *Détachement Central interministériel d'Intervention technique* (DCI), the Central Inter-ministerial Technical Intervention Detachment, will be handed over to the defence and security zones for greater responsive-

ness in the initial operations to deactivate improvised radioactive devices (so-called "dirty bombs").

Facilities for the hospital treatment of victims of a CRBN attack will be improved, and hospitals with approved emergency capability will gradually be equipped with permanent decontamination facilities.

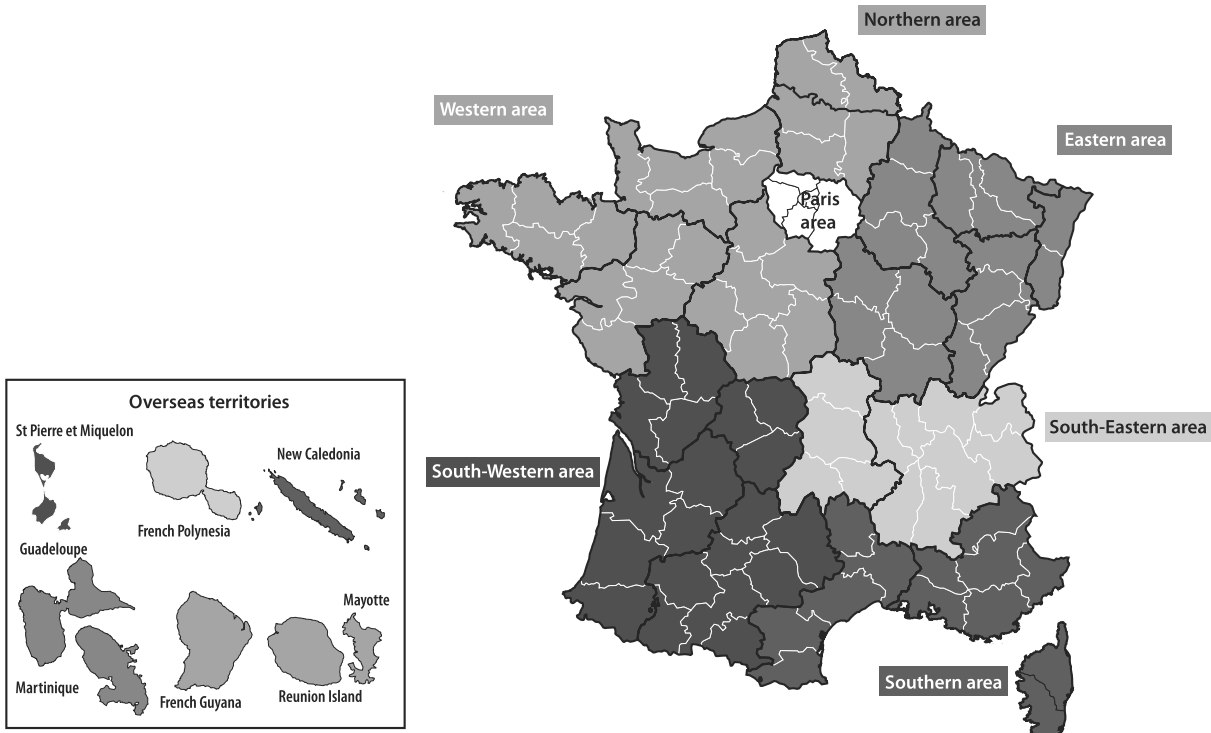
Research and development work on new means of identifying biological and chemical agents and explosives (particularly home-made devices) will continue.

Defence and security zones

Metropolitan France is organised into seven defence zones, which constitute the intermediate echelon between national and departmental level. The French overseas *départements* and territories (DOM-COM) are organised into five zones. These zones represent a level of co-ordination and action that draws a balance between the demands of proximity to the terrain and those of asset-sharing.

It is proposed that these should be renamed defence and security zones, that the scope of their powers should be extended and that their missions and resources should be adapted to the management of major crises.

Defence and security zones



Source: Ministry of Defence/Ministry of the Interior.

Protection of critical information systems

Faced with a growing threat, whether State-backed or otherwise, France must in the short term acquire reactive capability to protect the nation's information systems.

Early-warning systems will be developed to detect cyber attacks by setting up a detection centre in charge of the permanent monitoring of critical networks and implementation of appropriate defence mechanisms.

To combat the threat, greater use will be made of *security products and trust networks*. This in turn will require sufficient national capacity in the industry to master and develop very high-security products to protect State secrets, as well as a range of guaranteed "trusted products and services" for use by government agencies and services which will be made widely available to the business sector.

Regulatory provisions will also be introduced to ensure that electronic communications operators implement the technical and organisational measures necessary to protect their networks against the most serious failures and attacks. In this respect, the Internet will need to be considered as critical infrastructure and considerable effort will be made to improve its resilience.

A *new agency responsible for information systems security* (*agence de la sécurité des systèmes d'information*) will be set up to reinforce the coherence and capacity of State resources. Reporting to the Prime Minister and operating under the aegis of the General Secretariat for Defence and National Security (SGDSN), the agency will take over, and substantially expand, the staff and resources of the SGDN division currently responsible for this task. The agency will operate a centralised capability to detect and defend against cyber attacks. It will have the resources to sponsor the development of, and acquire, the security products essential to protect the Government's most sensitive networks. *The agency will also take on an advisory role to the private sector, particularly in areas of critical strategic importance, and will participate actively in the development of security for the information society*. The development of Internet sites dedicated to information system security and accessible to all will be one of its responsibilities.

More generally, the Government administration will enhance its expertise by increasing the numbers of specialised personnel in the ministries, creating a reservoir of competencies available to serve the needs of government departments and operators of critical infrastructures.

In view of the international dimension of the threats to communication networks, the agency will maintain close links with our main partners, particularly in Europe, and will encourage the development of a *Europe-wide* communication networks security policy.

A nationwide network of experts will also be established in the form of information system security observatories in the defence and security zones. These observatories will report to the zone Prefects and their principal tasks will include support (training, advice) to local government, organisation of networks and reporting early warning-signs of incidents.

Countering ballistic missile threats

At present only the major world powers possess ballistic missiles with sufficient range to reach Europe and France. It is already clear, however, that other powers will, over the course of the next few years, achieve possession of operational assets with equivalent capabilities. The spread of the necessary technology means that the probability of such proliferation increases with time.

— As part of its contribution to European and Atlantic solidarity, France will adopt an active *prevention* strategy designed to curb ballistic weapons proliferation, especially in the highest-risk zones. The strategy will be based on France's capability to *deter* any intent by another State to attack our vital interests using weapons of this type.

— France will also reinforce its *intelligence* and response capability. With this end in view, France will acquire a *detection and early-warning capability*, interoperable with that of our allies and partners. This capability will enable us to monitor the evolving ballistic threat, pinpoint missile launch origins in order to identify the instigator of the attack, and improve the public alert system. It will be based first on very long-range *radar pilot system with a view to initial operating capability in 2015*. In parallel, research and studies will be continued to pave the way for the launch, if possible in co-operation, of an advanced satellite detection programme. Our goal is to possess *a space based early warning system in 2020*. Taking into account the degree of technological complexity and risk associated with such a project, this programme will entail deployment and use of a probational satellite capability in the first half of the coming decade.

— Within the framework of the European Union and of the Atlantic Alliance, France will participate in combined efforts that may result in the deployment of an *active missile defence capability*. To this end, France will provide continued support for NATO-sponsored research to determine the global architecture of a system to defend the Atlantic Alliance against long-range ballistic missiles.

— Lastly, the authorities must make preparations to *mitigate damage* of any kind that may ensue as a result of missile attack on national territory, through a combination of response and protective measures, including alerting the public.

Detection and early warning

The early-warning capability is intended to detect and identify the nature of a ballistic missile launch as soon as possible after firing. A detection and early-warning system has *three objectives*:

— *Monitoring the proliferation of ballistic missiles*: missile test-firings are a good indicator of the technical and industrial maturity of proliferating countries. Detection and early-warning offer an independent assessment of the advancement of missile programmes and can be useful in characterising the technical elements of the threat.

— *Determining launch origin*: using trajectography data for the inbound missile, detection and early-warning can help to identify the aggressor and, where necessary, implement retaliatory measures. In so doing, it also reinforces the credibility of deterrence. It also offers the possibility of destroying hostile sites and missiles on the ground through the use of deep-strike capabilities.

Improving the public alert system: the flight time of a ballistic missile is normally a matter of minutes (around fifteen minutes over a range of 3,000 kilometres). The earliest possible detection of missile launch and determination of target area will allow for maximum use of the time available to alert potential target populations and implement the appropriate protective measures.

The early-warning capability relies on:

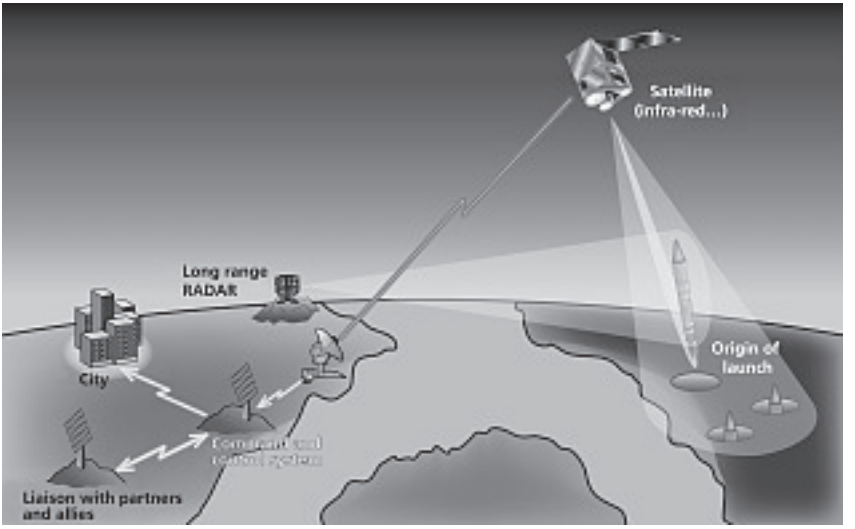
Space-based infrared detectors, able to detect the heat given off by the missile's engine during the powered phase immediately after launch; these detectors are mounted on geostationary satellites providing permanent surveillance;

— *Ground-based detectors* such as very long-range radar (range of the order of 3,000 kilometres), capable of detecting missiles even after their engines cut off.

— Space-based resources are designed primarily to detect long-range and intermediate-range ballistic missiles (from a range of 3,000 km upwards) with a fairly long thrust phase. Short-range missiles remain difficult to detect from space. *Space-based and ground-based assets are thus complementary*.

In view of the technical complexity of such a system, France has already embarked on research work. The SPIRALE (*Système Préparatoire Infra-Rouge pour l'ALErte*) early-warning demonstration programme consists of two micro-satellites to be launched by Ariane 5 in 2008. *The satellites will gather infrared images of terrestrial backgrounds*. The demonstration system will be followed by a precursor system for the detection and trajectography components.

Detection and early warning



Reinforcing civil protection capability to cope with major crises

Major crises, whether intentional in origin or otherwise, can affect whole populations, especially in the DOM-COM as a result of geographic factors. They may trigger massive displacements of populations, whether organised or spontaneous. Recent examples have suggested an order of magnitude (tens and sometimes hundreds of thousands). The issues raised by the evacuation of populations and its consequences, in terms of dealing with the victims, have been insufficiently addressed.

Plans will therefore be drawn up, with military support, under the auspices of the Ministry of Interior. They will include the pre-positioning on national territory of the logistics resources immediately necessary to cope with tens of thousands of evacuees.

In addition, an inter-ministerial approach to helicopter rescue missions will be adopted. Defence and Interior Ministries in particular, as well as other public and private operators (SAMU emergency medical response units, companies, etc.), own and maintain redundant helicopter capabilities. Rationalising these resources will generate cost reductions (training, support, alert, equipments, development, etc.) and optimise their use.

Large-scale natural or technological disasters

The recurrence of major events of increasing gravity has been confirmed over recent years, mainly as a result of population densification in high-risk areas. The likelihood of a major technological accident combined with a natural disaster is increasing. The risk is enhanced still further by the threat of attacks on critical facilities.

A crisis on this scale would have international repercussions. The European Union is working to acquire the means of effective solidarity, without calling into question the primary responsibility of Member States which will either benefit from or contribute to aid under the terms of European solidarity, as circumstances may dictate. In France's case, specific provision must be made for its overseas *départements* and territories (the DOM-COM), both because of their remoteness from Metropolitan France and their greater exposure to natural hazards.

The effects of a large-scale disaster affecting hundreds of thousands, perhaps even millions, of people, would be felt as follows:

— Immediately, in the form of risk to life and destruction of property and infrastructure;

— In its immediate aftermath, with implications for public order arising from the unstable situation faced by the population and the temptation to engage in looting;

— Consequences for health: diseases linked to the pollution caused by a technological accident or by a natural environment significantly degraded as a result of the disaster;

— Economic and social consequences: disruption of everyday life for millions of people, in terms of employment, transport, economic activity and social cohesion;

— Environmental consequences: pollution of large areas by toxic agents, rendering areas unsafe for long periods, with the difficulty of ultimately being unable to guarantee that affected areas and buildings are safe for human use.

As far as *anticipation* is concerned, the ability to forecast natural events depends on the physical nature of the events and on local circumstances and in some cases remains an impossibility. The authorities must, however, be able to rely on *a network of scientific specialists* identified in advance and familiar with crisis management procedures.

The development of forecasting and early-warning mechanisms is an imperative. Technological risk can be assessed—subject to an active prevention policy—but the event itself generally provides few advance warning-signs.

A determined policy of promoting *research* in these fields is essential for the future.

Prevention relies mainly on risk mitigation, population preparedness and crisis planning.

Unlike natural hazards, the risk of a technological disaster can be reduced at source by, for example, strict application of the "classified facility" (*installations classées pour la protection de l'environnement*, ICPE) system. The consequences of natural or technological disasters will be mitigated by the formulation of appropriate measures, written into natural or technological hazard prevention plans. Finally, *public information* to encourage widespread adoption of self-protective measures significantly diminishes injury and loss of life and should be reinforced.

Strengthening the resilience of the nation

PROTECTING CRITICAL INFRASTRUCTURE

The security policy for activities of strategic importance, launched in 2006, will be pursued vigorously. The policy covers twelve defined sectors and is intended to assess and rank risks, then take measures to address them. One of the essential aims of the policy is to determine which strategic sectors will require the most significant effort of protection in the years ahead, initially from operators and subsequently using the resources of the State if necessary.

Critical sectors

(Regulation of 2 June 2006)

Civil activities of the State – Judiciary activities – Military activities of the State – Food – Electronic communications, audiovisual and news media – Energy – Space and research – Finance – Water supply – Industry – Health – Transport

A number of major infrastructure resources, particularly for the transport of energy, information and goods, are trans-national. The security of such resources must be addressed coherently by the States and operators concerned. To this end, the French approach to strategic sectors will be presented to France's European partners in order to take forward initiatives launched by the European Union to establish common principles for critical infrastructure protection and promote the sharing of best practices.

Improving the public communication, information and alert mechanisms

Communication is an integral part of any national security strategy. Handling a major crisis requires, first and foremost, retaining the population's trust in the authorities. Silence on the part of the authorities, withholding of information, an appearance of improvised, unfocused communication, or messages that are exclusively defensive in tone, invariably add to a sense of anxiety which is inevitably passed on and amplified by the media.

The communication which accompanies a terrorist attack or the most severe natural or industrial disasters leaves a profound and lasting mark on collective memory as a result of the stress that such events engender. The first public reference to an event that threatens the continuity of normal life is therefore a key moment and must be the responsibility of the senior person responsible for handling the crisis. The next step is to lose no time in informing citizens as to the real nature of the event, how they should react, the objectives of government action and how they can contribute to their realisation.

Two levels of government communication must therefore be clearly distinguished:

— The political and strategic level of general communication;

— Communication aimed at those in the field.

Alerting and informing the public, along with communication, will be made central to the crisis management process.

Modernising the public alert system

First and foremost, France must have the means of informing the public rapidly. A powerful and robust alert network will be introduced, replacing the present system. The system will need to be fully modernised to make the most of the diversity of means now available: sirens, text messaging, e-mails, public bulletin boards in towns, railway stations, airports and on road and motorway networks. The potential of the Internet must also be exploited.

In addition, dedicated standalone means of communication (satellite phones, off-network radio-telephones, etc.) will be provided in case of total loss of electrical power supply.

Planning and professionalising crisis communication

In an environment characterised by a proliferation of messages, widely-scattered contacts and the instant flow of information from a

huge diversity of sources, the first problem is the legitimacy and credibility of the "official" message. Comments by so-called experts, the immediate broadcasting of raw images, the rapid succession of stories designed to capture the public's attention, make it all the harder for the population to understand the statements put out by the authorities. If it is to be effective in such circumstances, crisis communication will need to have been thought out and organised in advance.

A section on communication will therefore systematically feature in all crisis management planning. The "avian flu pandemic" plan already incorporates communication as an operational dimension in its own right, analysed and set out in detail in the same way as all the other actions included in the plan.

Planning will be accompanied by a joint effort to prepare for communication in an emergency. Plans are of little use if those who will be called upon to implement them lack a minimum understanding of the institutional and operational context of their implementation. A permanent *inter-ministerial network* of experts will be set up, whose members are used to working together, and who will be responsible, when the time comes, for implementing the planned measures.

National and area exercises to test the plans will bring together all those involved in crisis management, including representatives of the highest political authorities, the media, local elected officials and public and private operators.

The location from which the message is issued will also influence public perception of the crisis management as such. At national level, the political decision-makecharged with the strategic management of major crises will have access to facilities to issue full and informed public statements. Crisis operations centres will be provided with facilities to allow operational officials to address the population. At the local level, the necessary resources will be placed at the disposal of the representative of the State.

Developing inter-ministerial tools for broadcasting information before, during and after a crisis

France will at the earliest possible opportunity set up a *government Internet portal* to raise public awareness of risks and responses in the event of a crisis.

In addition, a *national call centre* will be established, with the task of providing information to the population on the cause of the event, advising those affected by the alert, answering questions and allaying concerns, calling on expert advice as necessary.

It is important to draw on other countries' experiences in this field, which shed light on how far citizens can be encouraged to prepare for

a crisis without unnecessarily fuelling anxiety. Internet sites dedicated to individual preparedness for crisis situations exist in most European countries.

Making the news media a key partner in the event of a crisis

The media nowadays are too often perceived by government agencies as likely to have a negative impact on crisis management. On the contrary, in situations where national security is at risk, journalists must be recognised as partners in the chain of crisis communication, independent yet responsible. As is the practice in the United Kingdom, journalists should be given the fullest possible information, as this will only help to improve the information that reaches the public.

This approach should prevail both before and during the crisis.

Before the event, journalists must have been provided with adequate and concrete information on the crisis management organisation and the resources available to the authorities, without breaching the necessary confidentiality which should surround certain mechanisms and responses. With the approval of media managers, media professionals will also be included in crisis exercises.

Informing the public about procedures and resources is likely to encourage the vigilance necessary as regards certain risks and an understanding of the measures taken by the State or the main operators. *It is always easier to deal with a vulnerable area of social or economic life when everyone knows of its existence.* This approach will enhance the resilience of our society and its capacity to deal with risks alongside the authorities and all their partners.

During the crisis, those in charge must take the initiative of explaining the key facts rapidly to those whose business it is to report them. The most seasoned media professionals are increasingly aware in advance or in real time of realities on the ground, or even of military or civil manoeuvres. The principle of a period of secrecy, if legitimately applicable, which lies at the heart of the decision-making process or of intelligence and action capabilities, must not become an obstacle to successful crisis management. The instantaneous broadcasting of information that is typical of crisis situations calls for other communication and information strategies as the crisis unfolds. Greater openness must be the rule, particularly as regards rescue or peace-keeping operations. Reliance on public means of information as part of the manoeuvre will be incorporated as such into the operation plan at every level, to a far greater degree than is currently the case.

Along similar lines, *a mechanism for dialogue at times of major crisis* will be established between predetermined contacts in government services, crisis management centres and the main media.

Finally, the management of the media concerned will be invited to take part in experience feedback analysis to improve the authorities' awareness of the effects and perception of their action.

Improving crisis management on French soil

Although in recent history France has not, unlike the United States, Spain or the United Kingdom, been faced with a major crisis on its soil, this fortunate circumstance could turn into a weakness if the authorities do not improve their collective preparedness for such events.

At central level

Significant progress has been made in recent years, particularly with the rethinking from 2001 onwards of the "Vigipirate" anti-terrorism plans. Government strategic planning capabilities nonetheless remain limited, incomplete and dispersed. The system is insufficiently co-ordinated and inadequately linked in to the national network at *préfecture* level.

This situation is perilous, because of the recurring characteristics of early XXIst century crises: instantaneous information, European and international interactions, impact not only on national land-space but also in the air, sea and cyber-space, simultaneity or chain-linking at several points around the country or the world, a multiplicity of parties concerned, both public and private.

A new organisation is therefore necessary in order to prepare and guide government action.

The principal orientations and governmental plans will be adopted by the *President* in the councils which he chairs. These plans will be drawn up by the *Prime Minister*, supported in this instance by the General Secretariat for Defence and National Security, which will co-ordinate the formulation and approval of governmental plans, involving all the ministries concerned.

The crisis management policy and strategy come under the authority of the President and the Prime Minister. It is their responsibility to organise political decision-making during a crisis. They must

be able to rely on a command organisation geared to major crises, guaranteeing real-time information on the progress of events and enabling them to direct government communication. The public, media and all those involved, in France and overseas, must be familiar with the existence of this organisation, which will be the natural point of entry into the crisis management structure for European and international contacts at the highest level.

The Minister of the Interior, who is responsible for domestic security and for civil security and protection, in the broader sense that these terms will be given in the Defence and Domestic Security Codes following reform of the ordinance of January 7, 1959 (see Chapter 3), will be responsible at the operational level for inter-ministerial management of crises on the French national territory. The Ministry's present resources will be supplemented by the creation of an *Inter-Ministerial Crisis Management Centre based in Place Beauvau*, within which all the Ministries concerned (Economy, Transport, Health, etc.) will be represented. The centre will network with the resources of the other ministries, particularly those responsible for foreign affairs, industry, transport and energy, and will ensure the coherence of civil and military responses in conjunction with the armed forces operational centre.

In terms of crisis preparation, the Ministry of the Interior will be responsible for plans dealing predominantly with public order and civil protection and security and will play a leading role in the formulation of plans to protect against terrorism on national soil.

The Ministry of the Interior will be provided for the purpose with a new directorate responsible for planning, reporting to the Secretary General of the Ministry (see Chapter 15). The directorate will act in close liaison with the Directorate General of the National Police, the Directorate General of the *Gendarmerie* and the Directorate of Civil Security on operational matters, and with the new Prospective and Strategy Delegation on medium and long-term crisis planning. The new directorate will be tasked with designing, developing, updating and monitoring plans in areas under the direct remit of the Minister of the Interior, and will provide the Ministry's contribution to governmental plans extending beyond that remit. It will steer the transfer of government planning to decentralised levels, as decided in council by the President and the Prime Minister, ensuring that such planning is adapted to the local level and monitoring its implementation. The directorate will also be tasked, with assisting of the ministries concerned, with formulating planning implementing instructions for the information of the Prefects and the use of local government. The directorate will rely in all its missions on the defence and security zone Prefects.

At decentralised level

Crisis management on national territory falls under the powers of the Prefects. *The defence and security zone Prefects* will have their powers extended to make them the first level of inter-ministerial decentralisation in terms of preparation for and management of major crises affecting national security.

The defence and security zones will perform the following main functions:

— Steering crisis forecasting and management;

— Collating information in crisis situations;

— Providing support to the departments on planning, exercises and training;

— Organising cross-border co-operation policy on civil security and protection.

Defence and security zone Prefects will also be given responsibility for steering a policy of organisation and harmonisation of all ministry reserves, in conjunction with the military authorities as regards the military reserves and in support of the département Prefects as regards local government reserves.

The co-ordination of civil and military resources in the defence and security zones will need to be stepped up.

Zone Prefects will be supported by military advisers, who will be the generals of the defence zones, under the direct command of the Chief of the Defence Staff.

The staffs of the zone Prefects and of the generals of the defence zones will be combined. Military planning resources will be incorporated into a single staff under the authority of the zone Prefects, so that government plans can be jointly applied at zone level across the country.

The generals of the defence zones will be empowered by the Chief of the Defence Staff to call upon the zones' regular military resources, for faster responsiveness in placing these resources at the Prefects' disposal in the event of a crisis.

In order to allow the inter-ministerial role of the zone Prefects its full scope of action, decentralised ministry organisations involved in crisis management will be aligned or harmonised at zone level.

Lastly, the Minister of the Interior will regularly convene a committee of defence and security zone prefects, with the Planning Directorate providing the secretariat.

Interoperability

Crisis management tools are insufficiently interoperable in technical terms at present. Interoperability will be enhanced and this applies in particular to the information, command and communication resources of the public security forces, the civil security forces and the armed forces. Establishing reliable links between the various agencies is key to the smooth running of crisis management, especially in the first hours after the response is triggered. The Inter-ministerial Secure Intranet System (ISIS) will be extended for this purpose to the entire decision-making and command chain in Metropolitan France in the near future.

Involvement of local government and operators

The effects of the decentralisation policy, and in particular the evolving relations between the State, operators in sectors of vital importance and local government agencies will need to be better understood and taken into account. As in the case of training, these actors will need to be more closely associated with planning. They are in possession of the competencies and the key resources, in the field of civil security for example. At the same time, the different legal schemes covering requisitions will be harmonised, in order to guarantee that, in times of crisis, the representatives of the State enjoy the full support of all the actors involved.

Training for crisis response

A coherent response to a major crisis also requires the various agencies involved in crisis response to receive regular training in joint action, at all levels. There is still significant progress to be made in this area, and in the analysis of experience feedback. Long-term inter-ministerial planning for such exercises will be put in place. The necessary financial resources will be identified. The feedback process will be formalised.

Particular attention will need to be paid to better training across the entire crisis management chain, from the strategic steering structures down to actors in the field. The personal involvement—even if only occasional—of senior political decision-makers or their representatives will be encouraged as an essential condition for the realism and effectiveness of such exercises. Local elected officials, who are often in the front line of disaster response, will also need to be closely associated.

Establishing objectives and operational contracts for the domestic and civil security structures and for the armed forces

Whatever the crisis scenario, the first land-based response is always carried out by the domestic and civil security structure. The armed forces complement this response, using their specific resources and know-how as requested by the civil power responsible for crisis management.

Thus the *domestic and civil security system* stands in the front line in dealing with all risks and threats on national territory. Should a major event occur, provision must exist for all resources in the vicinity, including the operational reserves, to be committed immediately and rapidly reinforced, where necessary, by special intervention units (RAID, GIGN, DCI, GIH) and by at least thirty *Gendarmerie* mobile units and ten Civil Security reinforcement columns equipped with CRBN protective gear. This will be set out in the *operational objectives* laid down for the domestic and civil security system as part of the civil and military planning of crisis management.

Similarly, *an operational contract of protection* applies to the armed forces on national territory. This is in addition to the general support missions provided by all the armed forces on national territory. It includes a land-based force capability of up to 10,000 soldiers, if necessary, deployable in a matter of days to contribute, at the request of the civilian authorities, first to the security of points of vital importance, and for land-based flows essential to the life of the country, as well as to control access to the national territory.

At the same time, the armed forces must also be able to provide reinforcement of the permanent air security posture, up to six operational patrols and four operational patrols specialised in combating low-speed aircraft. Reinforcement of the permanent maritime security posture requires the deployment of a frigate, of two mine-hunters and a maritime patrol aircraft on each of the three seaboards.

The Directorate-General of the Customs will act in co-ordination with the services concerned in the event of a crisis requiring increased surveillance, or even the closing of the borders. The Customs service will have the capacity to concentrate its forces rapidly at the most sensitive entry points, and will co-ordinate its maritime and air resources with the armed forces in order to ensure optimal national coverage.

In the overseas *départements* and territories (DOM-COM), co-ordination of civil and military resources will be strengthened and

forces will be reorganised according to the following principles (with no impact on *service militaire adapté*, SMA, vocational training units with military cadre):

— Redefinition of a predominantly air and sea force in each collectivity to carry out public service missions and combat all forms of trafficking;

— Establishing theatre resources in French Guyana, Réunion and New Caledonia capable of rapid intervention in the three zones, West Indies-French Guyana, Indian Ocean and Pacific Ocean respectively, in the event of a crisis (natural disaster, for example).

Gendarmerie and Civil Security resources will be adapted and reinforced as necessary, particularly as regards helicopters.

Crisis in the French overseas *départements* and territories (DOM-COM)

Over the next fifteen years, specific concerns will weigh on the defence and security of the DOM-COM, namely:

— The risk of natural disasters;

— The security of the Kourou space centre in French Guyana, vital to both France and Europe;

While all the *départements* and territories are not equally threatened, this type of event is one of the most influential factors determining the scale of government response.

The remoteness of the DOM-COM from Metropolitan France (7,000 km in the case of French Guyana, 8,000 km for Mayotte, 18,300 km for New Caledonia) may make the rapid projection of reinforcements, of both personnel and equipment, more problematic, and increase the difficulties of crisis management.

The probability of hostile action, particularly of a military nature, by a regional actor is considered to be much lower. The Kourou site is a special case, requiring specific resources.

Strengthening cooperation with European States

Crises may have cross-border impacts not only because of their nature (pandemic disease, for example), or the scale of their consequences, but also because any major crisis (terrorist attack, for example) carries an international dimension even if its effects are confined to France.

There is considerable margin for progress in terms of protecting European citizens, given existing practices and degrees of compartmentalisation.

It will be important to make use of all the mechanisms that EU Member States decide to implement under the terms of the solidarity clause in the Lisbon Treaty.

The precise terms of the co-ordination between States in the event of a major crisis will need to be clarified and made known to all concerned. France will appoint a *national co-ordinator*, who will be known to our partners and allies, to work with the decision-makers and officials in charge of crisis management.

Procedures for the co-ordination of crisis communication will need to be introduced by the European Union. The practice of staging European exercises will be developed in order to test the co-ordination of chains of command and national protection (and communication) capabilities in the event of a crisis affecting several countries, or in close proximity to our external borders.

Integrated management of operational co-operation at the European Union borders will also need to be improved, with the effort focused on Frontex, the EU agency for external border security.

In the area of civil security, France will support reinforcement of European capabilities for civil protection and fighting CRBN threats (see Chapter 4).

Main decisions relating to the protection of the population and territory

— Develop the surveillance of national spaces and those in which France has interests, including outer space.
— Significantly reinforce efforts to combat CRBN threats, in the field of detection, analysis and response as well as in the treatment of victims.
— Acquire active, in-depth cyber-defence capability, combining the intrinsic protection of systems, constant monitoring of critical networks and a rapid response in the event of attack.
— Acquire a detection and early-warning capability in order to counter the ballistic missile threat; the capability will be interoperable with that of our allies and partners and will rely on both radars and a space-based system.
— Develop a new strategy and modernise population alert and information systems and crisis communication systems.
— Substantially strengthen national planning and crisis management capability, with significant developments in the co-ordination of civil and military resources and improving the organisation of our co-ordination with our European neighbours.
— Set operational objectives for the domestic and civil security structure and an operational contract of protection for the armed forces, in order to cope with large-scale attacks and disasters that might take place on national territory; restrict the military presence in the DOM-COM to needs corresponding strictly to the missions of the armed forces and the Adapted Military Service; redeploy and, where necessary, reinforce *Gendarmerie* and civil security resources to guarantee continuity of public service in the areas concerned.