COUNCIL OF THE EUROPEAN UNION

Brussels, 8 April 2013

6090/10
ADD 9 EXT 1

ENFOPOL 38
PROCIV 15

PARTIAL DECLASSIFICATION

of document:	6090/10 ADD 9 RESTREINT UE/EU RESTRICTED
dated:	5 March 2010
new status:	Public
Subject:	Second Round of Peer Evaluation Preparedness and consequence management in the event of a terrorist attack

Delegations will find attached the partially declassified version of the above-mentioned document.

ANNEX

COUNCIL OF THE EUROPEAN UNION

Brussels, 5 March 2010

6090/10
ADD 9 EXT 1 (08.04.2013)

ENFOPOL 38
PROCIV 15

ADDENDUM TO THE NOTE

from :	The Council General Secretariat
to :	Working Party on Terrorism
Subject :	Second Round of Peer Evaluation Preparedness and consequence management in the event of a terrorist attack

Delegations will find enclosed the report of the evaluation mission in **France** (19-21 November 2008) in the framework of the above-mentioned round of peer evaluation.

1. EXECUTIVE SUMMARY

- In the framework of the second round of peer evaluation covering "Preparedness and consequence management in case of a terrorist attack" an evaluation visit was made to France from 19 to 21 November 2008.

- Threat evaluation

  Owing to its involvement in the international scene and its historical links with the Muslim world, France has long been exposed to the terrorist threat (1970s). For some decades it has also suffered internal terrorism, whether due to political extremism or to separatism. The threat has continued to the present day. AQIM currently regards France as being its main enemy, after the Algerian government. Because of France's commitment to the international community, the reinforcement of its military contingent in Afghanistan, the terrorist threat both to national territory and to French interests abroad is high. The warning and alert VIGIPIRATE plan has accordingly been kept at red level for several years now.

- Brief description of institutions

  The impression gained from the institutions that were presented and visited is an entirely positive one. All aspects of crisis management – threat assessment, planning and organisation of emergency arrangements – appeared to be very well covered. Coordination of the institutions is ensured by the centralisation of the system and the specific situations managed by appropriate bodies.

  The Interior Ministry is the ministry for managing crises in France, especially crises that may arise from terrorist activities. It is also responsible for domestic threat assessment. The high-level planning of crisis management is carried out by the Prime Minster, with the assistance of the General Secretariat for National Defence (SGDN), which belongs to the Prime Minister's offices.

  The city of Paris and neighbouring departments come under the *Prefecture de Police* Headquarters, which is an administration covered by specific arrangements owing to the concentration of powers on this particular geographical area.

The Civil Security Directorate is in charge of organising assistance at national level, whatever the cause of the crisis. It is one of the directorates of the Interior Ministry. Two police forces, one with civilian status (national police), the other with military status (national gendarmerie) have jurisdiction in French territory. As from 1 January 2009 the national gendarmerie will be an integral part of the Interior Ministry, while retaining its military status. Up to now it has only been operationally attached to the Ministry. There is a territorial allocation of responsibility between the two forces: the national police have more responsibilities in urban areas, the national gendermerie in the rural areas.

The overall arrangement appeared to be very coherent and highly adaptable.

- The main recommendations resulting from this evaluation mission focus on the following areas:

NOT DECLASSIFIED

2. ARRANGEMENTS IN THE EVENT OF A TERRORIST ATTACK

2.1. Structures and organisational framework of National Crisis Centres

Each ministry has an operational centre for managing crises in its own sector and a crisis unit may also be set up at the President or Prime minister level. The centres are interconnected and they cooperate in the event of a crisis.

The Interior Ministry is the one with particular responsibility for crisis management in France. To do this, it has a number of operational centres under it: the Beauvau Operational Centre (COB), so named from the place where it is located; the Interministerial Operational Crisis Management Centre (COGIC), which comes under the Civil Security Directorate (DSC); and the Information and Operations Centre of the National Gendarmerie (CROGEND), which comes under the Directorate-General of the National Gendarmerie (DGGN). This keeps the DGGN constantly informed about the activities of the Gendarmerie. At the request of the Prime Minister, the Interior Minister may also set up and coordinate an interministerial crisis unit (CIC). The various operational centres have a number of back up structures for cases where the functioning of some of them is disrupted.

- The COB, which reports to the office of the National Police Director-General (DGPN), is responsible for crisis monitoring and management as regards action by the police. If attacks took place, the Counter-Terrorism Coordination Unit (UCLAT) would play a major role within the COB by providing operational coordination between the on-the-ground personnel of the counter-terrorism directorates and services. The COB is a non-permanent structure activated in a major crisis by the DGPN. As well as managing the police forces, it is responsible for centralising intelligence, analysing it, and distributing summaries of the information gathered to the authorities concerned.

  In crisis situations other than those where the COB is involved, internal security information is gathered, verified, summarised and communicated to the DGPN by the Operational Surveillance Service of the National Police Force (SVOPN), which has been part of its Office since 1 April 2006.

The SVOPN operates 24/7. This is the service which receives the order from the DGPN to activate and operate the COB within a maximum of two hours.

The following, among others, are represented within the COB:

- Paris Police Headquarters (PP)
- Civil Security Directorate (DSC)
- Central Directorate of the Criminal Police (DCPJ)
- Directorate-General of the National Gendarmerie (DGGN)
- Central Public Security Directorate (DCSP)
- Central Internal Intelligence Directorate (DCRI)
- Central Border Police Directorate (DCPAF)
- Central Directorate of the *Compagnies Républicaines de Sécurité* (riot police) (DCCRS)
- Air Force

Thus there are effective links via the COB between all the police and security forces that may be called upon to act in French territory [1] in the event of a crisis. The COB has been activated several times in connection with public order issues (urban violence, major events, large demonstrations). As regards terrorism, it has only been activated for exercises (in 2007 for the PIRAIR, PIRATOME and BIOTOX exercises and in 2008 for the PIRANET exercise).

- The COGIC is the permanent operational centre for the Civil Security Directorate. Working round the clock, it will monitor and manage a crisis at the level of all the emergency services until the situation returns to normal. It is in contact with the coordination centres of any other ministries that may have responsibilities in the management of a crisis (health, economy, transport, defence and foreign affairs). Its work is focussed on the emergency services and does not concern the investigative services.

[1] In the event of crises affecting French nationals or interests abroad, the Operational Centre of the Foreign Affairs Ministry is activated.

The COGIC is a strategic tool designed to facilitate the exercise of governmental authority in the context of this type of mission. It carries out continuous surveillance of the civil security operations over which it has a monopoly. It is the pivot of the operational chain between the national level and the local levels as regards the circulation of information and the coordination of operations. The COGIC has a National Advisory Unit (CNC) whose purpose is mainly to provide the emergency services with the necessary advice so ensure that they do not destroy any items of evidence in the course of their action.

- The CIC is set up by the Minister responsible for crisis management. In a particularly serious crisis, the CIC may be chaired by the Prime Minister or the President of the Republic. In the event of a terrorist attack, the CIC will normally be set up and attached to the Private Office of the Interior Minister. Where French nationals are taken hostage abroad, the CIC is normally attached to the Foreign Affairs Ministry. The Interior Ministry also has a coordinating role to play when a crisis goes beyond the sphere of competence of a particular ministry. Its duty is to ensure the operational continuity of government action. To achieve this, the CIC is also in contact with the main economic operators.

2.2. National arrangements in the event of a terrorist attack

In the event of a terrorist threat or attack, the French authorities' response is based on the activation of prevention, intervention and assistance plans. These are implemented by a centralised and clearly identified chain of command.

The action of the investigative services proceeds alongside the implementation of these plans. To ensure efficient deployment, their action too is organised beforehand.

2.2.1. Prevention, intervention and assistance plans

2.2.1.1. VIGIPIRATE

a) Origin

The warning and alert VIGIPIRATE plan and its various extensions are interministerial arrangements under the control of the General Secretariat for National Defence (SGDN). The SGDN is a Prime Ministerial office which assists the Prime Minister in fulfilling his defence and national security responsibilities. His many duties include prevention and preparing the State for major crises and hazards. The SGDN is responsible for drawing up a national security plan and ensuring the consistency of the policy of training and exercises in this area.

b) Description

The core of France counter-terrorism arrangements is the VIGIPIRATE plan and its various extensions. The plan was devised in 1978 with the dual aim of protecting people, infrastructure and institutions while preparing responses to any attack.

The VIGIPIRATE plan's general aim of deterring and preventing terrorist activity is backed up by the various PIRATE intervention plans, each of which is geared to a particular type of threat. PIRATE intervention plans are activated by the Prime Minister in the event of a specific terrorist threat or actual attack using a particular method:

– PIRATOME for nuclear or radiological materials
– PIRATOX for a toxic chemical product
– BIOTOX for a pathogenic biological agent
– PIRANET for an attack on information systems
– PIRATE-MER for dealing with maritime terrorism
– PIRATAIR-INTRUSAIR against air terrorism
– METROPIRATE in the event of attacks on urban public transport
– PIRATE-EXT in the event of threats or attacks against French nationals or interests abroad

These intervention plans set out a structure for crisis management and information-processing, as well as the steps to be taken by civil and military authorities and the main operators (mainly in the transport, energy and communications sectors). The idea of bringing PIRATOME, PIRATOX and BIOTOX plans together in a single plan is currently being studied. The initial threat is sometimes hard to identify and many of the response methods are common to all of them.

The latest version of the VIGIPIRATE plan (November 2006) is based on the assumption that the terrorist threat must be regarded as permanent. It sets out the basic measures to be applied in all circumstances, even where there are no signs of a threat. The plan comprises four levels of alert, which are made public. These are aimed at a number of security objectives:

- yellow: seeks to promote increased vigilance where there is a general threat with a minimum of disruption to normal activity;
- orange: seeks to prevent the risk of credible terrorist action by imposing slight constraints on normal activity;
- red: seeks to prevent the highly probable risk of a terrorist attack by putting in place appropriate measures involving constraints on countrywide activity;
- scarlet: seeks to prevent a definite threat of major attacks, whether simultaneous or not, with the implementation of highly restrictive measures.

While the alert levels are made public, this is not the case with the protection measures that are taken within each level and are themselves classified. And the fact that a particular alert level is selected does not mean that all the measures corresponding to it will be carried out. This is a strategic tool that can be adjusted case-by-case according to the locality and the concerned threat, to select security measures that will be applied by the Prefects and by the major operators (i.e. in the energy, transport and communications sectors). Partnership with these main operators is essential to the implementation of measures under the VIGIPIRATE plans. The main operators have an operator's security plan, for their entire activity, and specific protection plans for the protection of their critical infrastructures and assets. All these plans take into account the measures of the VIGIPIRATE plan, consistent with the sector specific risk assessments lead by the ministry in charge. The measures are approved by the Prime Minister and communicated by the SGDN to the authorities responsible for implementing them. Thus there is infinite scope for variation. Moreover, it is because of this scope for adjustment and variation that a high alert level can be maintained over a long period (there has been a red-level alert in France since the London attacks in 2005).

c) Implementation mechanism

Threat assessment is the basic element in applying the VIGIPIRATE plan. Each alert level is decided on the basis of a threat-assessment level. The choice of alert level is a political decision taken by the Prime Minister and the President of the Republic.

Domestic threat assessment is essentially the responsibility of the Interior Ministry, and in particular the Counter-Terrorism Coordination Unit (UCLAT). The UCLAT is a DGPN department responsible for the operational coordination of the services that may be required to play a part in the fight against terrorism.

– The threat assessment made by the UCLAT

To carry out its tasks of coordinating services and assessing threats, the UCLAT brings together some or all of the following services once a week, but more often if necessary:

– Internal Intelligence Central Directorate (DCRI)
– Paris Police Special Branch (DRPP)
– Technical International Police Cooperation Department (SCTIP)
– Directorate-General for External Security (DGSE)
– Military Intelligence Directorate (DRM)
– Defence Protection and Security Directorate (DPSD)
– Operational Air Force Command (CDAOA)
– National Directorate for Customs Intelligence and Investigations (DNRED)
– VIP Security (SPHP)
– Border and Immigration Police (DCPAF)
– Central Public Security Directorate (uniformed police) (DCSP)
– Gendarmerie (DGGN)
– Paris Police Criminal Investigation Department (PP-PJ)
– Central Directorate of the Criminal Police (DCPJ)
– Search, Assistance, Intervention and Deterrence Unit (RAID)

It also has a number of liaison officers posted abroad (Germany, Belgium, Spain, Italy, United Kingdom) and hosts liaison officers from these countries in its own offices.

The UCLAT is also the contact point for a number of international organisations (liaison offices network, PWGT, G8 contact point).

Being at the centre of the intelligence flow means that the UCLAT is able to make a precise threat assessment on a weekly basis (but also on request) and present it to the Interior Minister, who can then submit it to the Prime Minister and thus help establish the alert level that is eventually adopted for the VIGIPIRATE plan.

2.2.1.2. The ORSEC plan

The ORSEC plan (Organisation of Civil Security Response) is actually a set of plans prepared by the Interior Ministry's Civil Security Directorate (DSC). It is adapted to each territorial level and primarily concerns the organisation of assistance to populations in various circumstances (floods, heatwaves and cold spells, earthquakes, major accidents, natural or technological disasters, attacks, etc.). Its sphere of application is therefore different from but complementary to that of the VIGIPIRATE plans.

The ORSEC plan was reformed in 2005 [1]. It has three main elements:

– Inter-service identification of the risks and effects of threats
– Operational arrangement with both general and specific provisions
– Procedures for preparing and carrying out exercises

The general idea behind the ORSEC plan is to return the situation to normal as soon as possible.

2.2.2. Chain of command responsible for implementing the plans

The administrative organisation of the French services is highly centralised and has a clear chain of command.

The Interior Minister is the chief crisis manager in the event of a nationwide crisis. His action is communicated throughout the territory by the Defence Zone Prefects and the Department Prefects.

[1] Modernisation law and Decree No 2005-1157.

France has seven defence zones each of which covers a number of departments. The defence zone is a specialised level that comes between the central government and the department.

At the head of the defence zone there is the Zone Prefect, who is also the Regional Prefect and the Prefect of the central department of the defence zone. As regards crisis management and the organisation of assistance, the defence zone is the level that is most often called upon (although the ORSEC plan can also be triggered by the Department Prefect). One of the functions of the defence zone is to coordinate the civil security resources of all the departments in the area it covers. This makes it possible to increase the resources available to each department for preventing and managing crises whose scale goes beyond the territory of any one department in the zone. The defence zone is also the level at which there may be coordination with military resources.

In the case of the Paris region, all police and emergency services come under the direct authority of the Prefect of Police of Paris, who is also the Prefect of the Paris defence zone, which covers the eight departments of the Paris region.

If an incident occurs in Paris, the Prefect of Police of Paris – as Defence Zone Prefect – is in charge of the various aspects of managing the crisis. If an incident occurs in the provinces, the crisis management is led by the Defence Zone Prefect or, more rarely, the Department Prefect.

2.2.3. Planned action of the investigative services in the event of a terrorist attack

In the event of a terrorist attack, the judicial authorities systematically refer the case to the Central Directorate of the Criminal Police (DCPJ). If the attack takes place within the jurisdiction of the Paris Police Headquarters, the Counter-Terrorism Section of the Police Headquarters (SAT/PP) will be the territorially competent service. The judicial authority may also refer the case at the same time to the Internal Intelligence Central Directorate (DCRI)[1].

In the event of a CBRN terrorist attack the Central Inter-Ministerial Unit (DCI) has to intervene.

[1] The DCRI was set up on 1 July 2008 on the basis of the DST (Counter-Intelligence Agency) and the DCRG (Central General Intelligence Directorate). These last two services have since been dissolved.

During the evaluation mission we were given a presentation of the planning that underlies the action taken by the DCPJ and the SAT/PP. We also received some information about the action taken by the DCI.

2.2.3.1. Planning of DCPJ action:

Following the London bombings of July 2005, the DCPJ has made far-reaching changes in its response capability in the event of a terrorist attack in French territory. This has been done in two major areas:

– the creation of an "attack response capability" involving a crisis command post (CP) and workshops;
– the introduction of an electronic toll free number "green telephone line".

(a) The DCPJ's "attack response capability":

In this context the action taken by the criminal police will be coordinated at three levels (central, territorial and crimescene).

– At national level, setting up of a single crisis CP comprising eight topic-related workshops.
  - Findings and technical and scientific police
  - Victims
  - Witnesses
  - Intelligence and information-gathering
  - Checking of evidence, testimony and intelligence
  - Relations with foreign services
  - Hearings and searches
  - Centralisation of the procedure

– At territorial level (regional or inter-regional service), setting up of a crisis CP with an identical organisation (the same eight workshops) to that of the national crisis CP. A number of territorial CPs can be set up in the event of multiple attacks at various places in the territory. The identical nature of the facilities will make it easier for the central CP to use the information.

– At local level, setting up of one or more operational CPs (one per crime scene). This covers the case of attacks that take place simultaneously or in quick succession or at different locations. At local level only the "Findings and technical and scientific police", "Victims" and "Witnesses" workshops are put in place. These convey the information up to the territorial level, which in turn provides for interchange with the national level.

  This arrangement enables a consistent, pre-established response to be made to any type of attack that may occur and facilitates the initiation of investigations. The task specialisation saves time and makes the overall conduct of the operation more effective.

(b) Electronic toll free number

The Interior Minister or the DGPN may at any time authorise the opening of such line and of a website for receiving testimony about the events that have taken place. All information obtained in this way is recorded in a national database known as the "attack incident-book application". It is then processed and used by the "Intelligence and information-gathering" and "Checking of evidence, testimony and intelligence" workshops that are set up at local and territorial level. This allocation of tasks enables investigators at the crime scenes to concentrate exclusively on front-line work.

2.2.3.2. Example of the management of the consequences of an attack within the jurisdiction of the Paris Police Headquarters; action taken by the Counter-Terrorism Section of the Police Headquarters (SAT/PP):

In the event of a terrorist attack in the area covered by the Prefecture of Police of Paris, the body with territorial jurisdiction to intervene is the SAT/PP.

For this purpose, an overall study was made by all the services of the Prefecture of Police. It followed two broad lines:

– Attack-response plans
– Specific methods

(a) Attack-response plans

These involve a combination of emergency plans and the "multiple attacks" plan. The "multiple attacks" plan was drawn up following the experience of the London bombings in 2005. It was finalised with the other services that have to intervene at an attack scene, and in particular:

– the firemen responsible for assistance to the victims;
– the central laboratory of the Police Headquarters responsible for mine clearance and for handling explosives;
– the Public Order and Traffic Directorate has particular responsibility for ensuring the security of premises, clearing routes to hospitals, and organising the parking in pre-arranged areas of vehicles used by the services attending the attack sites.

The operation of the "multiple attacks" plan is synchronised with the "red alpha" plans and the "yellow" plan, which are emergency-service plans.

The provision of assistance under these plans is made easier by the existence of a network of CCTV cameras, of which there are between 300 and 500. This is not enough, however, to cover the whole of the capital.

- emergency-service plans

– The alpha red plan is a "multiple attacks" version of the red plan used by the fire brigade in response to disasters or large-scale accidents. It specifies in detail the deployment of the emergency services and also the other bodies involved.

  Once the firefighters have intervened, uniformed police officers set up a security cordon which is extended gradually as the emergency services arrive. Inside the cordon, the firefighters take command of the whole area during the administration of emergency care to the victims. After the emergency care stage, the Criminal Police will take responsibility for the area inside that perimeter. The site of the attack is delimited inside the security cordon; this area is then known as the security perimeter. Within the security perimeter and in parallel with the intervention of the firefighters, the bomb-disposal experts secure the area, aiming in particular to prevent any further attacks and the firefighters proceed to eliminate any CBRN risk.

Surviving victims are removed from the site of the attack and directed towards a specific point i.e. the Victim Gathering Zone, manned by police officers who are responsible for their identification.

One of the key ideas underlying the alpha red plan is centralised command (all the mobile CPs of the intervening services assemble in the same place) on the site of the attack. Centralisation allows for better use of the resources deployed and simplifies the assignment of staff and demarcation of the routes in and out i.e. the access and evacuation zones. This kind of coordination facilitates the work of the Criminal Police because the emergency services take account of the need to preserve the scene of the crime, the injured victims can be identified quickly as can the hospitals to which they are sent.

– The yellow plan is a variant of the red plan and covers use of a CBRN product. In addition to the provisions of the red plan, it envisages putting in place decontamination chains and police working on the site of the attack wearing protective CBRN clothing.

The yellow plan distinguishes three distinct action zones; the exclusion zone which corresponds to the pollution zone, the controlled zone which allows the deployment of decontamination measures and the support zone which constitutes the alpha red plan described above.

- The "multiple attack" plan of the Paris Police Criminal Investigation Department (PP - PJ)

The SAT/PP is a unit of the PP - PJ. Together with three other sections responsible for common law matters, it makes up the crime squad of the PP - PJ. In the event of a terrorist attack, by activating the multiple-attack plan eight departments of the PP - PJ, i.e. one thousand detectives, will be mobilised around Paris. The multiple-attack plan essentially corresponds to the Criminal Police's attack response capability examined above. The methods for implementation are as follows:

(b) Specific tools

- Dealing with victims

A terrorist attack, in particular multiple attacks, would pose the problems of counting and identifying victims.

The solution used to count victims is the SINUS system (standardised digital information system). Each victim is given a bar-coded bracelet. Computer activation of that bracelet automatically creates a file in a specific database. Initially such files do not contain information and serve only to count victims. Later on, as data is progressively entered in the files, the SINUS system can serve as a tool for victim identification. This database can be consulted by all the intervening services and administrative authorities.

The solution used to identify victims is the activation of the UPIVC (Police Unit for Victim Disaster Identification). This Unit is made up of an ante mortem team and a post mortem team.
The ante mortem team collects identification data on potential victims and the post mortem team works on the bodies discovered at the site of the attack. Used together, the data can result in victim identification. Once the death-toll is over ten, the UPIVC automatically gets involved.

- Specific investigation method

When the firefighters leave, command of the site of the attack reverts to the Criminal Police. The Forensic Services (*identité judiciaire*) map out the zone as a grid, and access is restricted to persons in crime scene technician's clothing. This method aims to return the site of the attack to an acceptable working size, and each square in the grid becomes an action zone for the team. The numbering of the items placed under seal follows an exceptionally precise protocol to avoid any confusion.

- Information management

Information management is based on the methods already described in relation to the Criminal Police. An Internet site, a toll free number (green telephone number) and the "attack incident-book" application are set up.

- Training

In the event of multiple attacks, terrorism specialists cannot conduct the preliminary investigations on their own. Consequently, all Criminal Police detectives are trained in the specific investigation techniques and methodology envisaged in these cases. Particular attention needs to be paid to investigative work; mapping out the site of the attack as a grid and working together with officials and experts from other administrative authorities.

Furthermore, training on wearing protective CBRN clothing and working in a contaminated environment is identified as one of the priorities of the training plan for Crime Squad officials.

2.2.3.3. Role of the DCI

The DCI was set up in March 1995. One of its tasks is to intervene if there is a risk of an attack from a device which might contain CBRN materials. The DCI's work is done before the explosion and the unit is not responsible for intervening after a CBRN-type attack[1]. Its role is to look for, locate, diagnose and neutralise the suspect device. This is an interministerial body, the command of which was entrusted to the Head of the RAID by joint decision of the Interior and Defence Ministries, acting on a proposal of the SGDN.

The DCI brings together staff from:
– the Ministry of the Interior
– the Ministry of Defence
– the Ministry of Economy and Finance (Atomic Energy Commission) and
– the Ministry of Health.

The DCI assesses the threat posed by the device and proposes appropriate technical solutions to solve the problem to the Prefect in charge of the crisis. The DCI regularly participates in UCLAT meetings to assess the CBRN threat.

[1] In the event of a CBRN attack, the entire intervention doctrine is covered in a circular. The first line of intervention is set up locally by the departments of the police, gendarmerie, emergency medical assistance and firefighters. This doctrine focuses on the rapidity of intervention. A second line of intervention is subsequently made up of back-up support sent by the defence zone and a third line by the use of national resources. Those national resources are primarily units made up of the national gendarmerie and civil defence.

2.3. Competences of the national crisis centres for potential cross-border targets for terrorist attacks

The operational centres do not treat cross-border targets any differently from national targets. The operational centres in the ministries have the power to manage a crisis affecting this type of infrastructure on national territory. This is also true of the COGIC.

Nevertheless, particular attention is paid to cross-border road and rail tunnels. Bilateral security committees have been set up and local relations play a part in assessing the risk faced by cross-border targets. As part of preparedness for a crisis or terrorist attack, designated contact points exist and bilateral meetings are held regularly via the diplomatic chain and specialised networks.

Major cross-border exercises, focusing mainly on transport infrastructure, have been conducted in cooperation with Germany and the United Kingdom. In addition, local cross-border exercises are conducted on regular basis.

More generally, provision is made for cooperation with neighbouring countries in bilateral agreements and cross-border cooperation is also organised at operational level.

To a certain extent, air space may also be considered a cross-border target. Consequently, to facilitate implementation of the PIRATAIR-INTRUSAIR plan against air terrorism, and given the specific nature of the threat which requires a rapid reaction, bilateral agreements have been concluded with certain neighbouring countries (Spain, Switzerland, Belgium, Italy, United Kingdom) or are being negotiated (Germany, Luxembourg).

2.4. Rules of internal communication in the event of a terrorist attack

NOT DECLASSIFIED

NOT DECLASSIFIED

NOT DECLASSIFIED

3. TRAINING/EXERCISES FOR TESTING THE NATIONAL CRISIS CENTRES AND COMMUNICATION SYSTEMS IN THE EVENT OF A TERRORIST ATTACK

The SGDN at interministerial level, the Ministry of the Interior, the Ministry of Foreign and European Affairs and the Ministry of Defence test, supervise and maintain the systems that they implement.

Policy on exercises and training for the fight against terrorism is defined by the Prime Minister. It provides for the organisation of exercises and/or training by the various levels concerned, from the Prime Minister's Office to the local units.

- **International exercises**

The French authorities take part in European exercises twice a year on average. Some cross-border exercises are also carried out, with Germany and the UK (blue current 08).

- **National exercises**

Through the major exercises established by the Prime Minister's Office, the SGDN assesses the appropriateness of counter-terrorism planning. The SGDN is responsible, together with all participating ministries, for drafting the scenarios for crisis management exercises. These are carried out at the level of ministerial offices and central State departments. Sometimes they involve some of the staff on the ground. In 2007, 90 % of the five exercises carried out in this context incorporated a terrorism aspect.

As regards communication systems, these major exercises deploy ministries' operational centre level organisations and the ISIS system. They involve communication tools that allow nominal operation of alert chains and information feedback chains from local to central level.
All the major exercises thus provide opportunities to test the communication and information tools set up for crisis management.

The experience drawn from these exercises makes it possible to update the intervention plans, which are also updated when the threat, regulatory context or economic infrastructures change.

All those involved centrally (ministerial offices, directorates-general) take part in the debriefing immediately after each simulation. Two months later, participants in the central game and the local game are invited to a final debriefing meeting at SGDN.

- **Defence Zone exercises**

These exercises are established by Defence Zone Prefects. Their purposes include training departments to work with the Defence Zone level. They mainly involve the emergency services. In 2007, 17 exercises were organised. They dealt with a very wide range of themes including pandemics and winter storms but 50 % of them included a CBRN element.

- **Departmental exercises**

These take place in accordance with plans drawn up yearly in a circular from the DSC addressed to Prefects. In 2007, 309 emergency exercises were organised, 25 % of which included a CBRN element.

4. SOFT TARGETS

The concept of a *soft target* is used in France and particularly concerns public gathering places. However, no special status is assigned to the "soft target" concept. The security of targets is ensured through the VIGIPIRATE plan. The numerous possible versions of the plan at different territorial levels allow it to be constantly adapted both to events occurring locally and to the evolution of the threat.

Under this plan several deterrent measures, such as increasing patrols and controls, are applied in places where large populations are concentrated or pass through. Keeping the VIGIPIRATE plan at red level facilitates the involvement of soldiers to reinforce police patrols in those places. The soldiers remain under the responsibility of the civilian forces accompanying them in the mission framework. Their presence appears to be welcomed by public opinion. In June 2008, a plan for specific intervention in the event of a threat or attack on public transport networks in urban areas (METROPIRATE) was finalised by the SGDN. It draws on the lessons of the attacks in Paris in 1995, in Madrid in 2004 and in London in 2005.

Substantial efforts have been made to carry out exercises in this field and to raise public awareness as to how to behave in the event of threats or attacks.

There are no national or local lists itemising the soft targets; France's position is a pragmatic one that takes account of a group of criteria that can change fast. There is no dedicated organisation to deal with threats on soft targets. The threat is considered at a general level, with awareness that soft targets have a favoured position in terrorists' selection of targets for attack.

5. GOOD PRACTICES

- Excellent upstream crisis management system through threat assessment carried out by UCLAT. That threat assessment, which involves all the services concerned, is essential to the process of establishing the threat level for the implementation of the VIGIPIRATE plan.

- Taken together, the VIGIPIRATE range of intervention plans created under the aegis of the SGDN fully cover the spectrum of the terrorist threat.

- The centralising of a clearly identified hierarchical chain seems particularly effective. The task of manager and coordinator of the Defence Zone Prefect, in the event of a crisis in their area of responsibility, represents a useful mechanism.

- The way in which the Prefecture of Police operates is perfectly fitted to the scale of the threat and the specific features of a territory such as the Paris Defence Zone.

- There is a clear distribution of tasks between the ORSEC plan and the VIGIPIRATE plans.

- The regular updating of the various plans on the basis of the outcomes of the exercises and of the evolution of the threat contributes to their effectiveness.

- The CBRN threat is very well covered in terms of both preventive intervention and intervention following an attack.

- By rationalising and providing a framework for the investigators, the "attack response capability" put in place by the DCPJ facilitates the progress of the critical initial phases of investigation after a terrorist attack has taken place.

- There is a real public-private partnership, with the main (telecommunications, transport and energy) operators very involved. At both planning and implementation levels of the exercises the partnership is based on constant communication.

6. RECOMMENDATIONS

NOT DECLASSIFIED

NOT DECLASSIFIED

7. ANNEX

7.1. Presentations were made by the following institutions

Ministry of the Interior

- UCLAT (counterterrorism coordination unit)
- COB (Beauvau Operational Centre)
- SICOP (National Police Information Office)
- Criminal Police Department/(Sub-directorate for the fight against terrorism)
- SAT/PP (Counterterrorism section of the Paris Police Headquarters)
- Directorate General of the National Gendarmerie

Paris Police Headquarters

- crisis room
- crisis management

General Secretariat for National Defence (SGDN)

- Emergency plans
- Interministerial crisis management
- Governmental communications management

Civil Protection Department

- Interministerial Operational Crisis Management Centre (COGIC)

7.2. Speakers

UCLAT (counterterrorism coordination unit)

NOT DECLASSIFIED

SICOP (National Police Information Office)

NOT DECLASSIFIED

COB (Beauvau Operational Centre)

NOT DECLASSIFIED

Directorate General of the National Gendarmerie

NOT DECLASSIFIED

Criminal Police Department/(Sub-directorate for the fight against terrorism)

NOT DECLASSIFIED

SAT/PP (Counterterrorism section of the Paris Police Headquarters)

NOT DECLASSIFIED

Paris Police Headquarters

NOT DECLASSIFIED

General Secretariat for National Defence (SGDN)

NOT DECLASSIFIED

NOT DECLASSIFIED

Civil Protection Department

NOT DECLASSIFIED

7.3. Expert team

Council General Secretariat

NOT DECLASSIFIED

Police and Customs Cooperation Unit – DG Justice and Home Affairs

Commission

NOT DECLASSIFIED

DG JLS – Directorate D – Unit D1

Europol

NOT DECLASSIFIED

Serious Crime Department – Counter Terrorism

Portugal

NOT DECLASSIFIED

Security information department

Romania

NOT DECLASSIFIED

Ministry of the Interior