

TACKLING TERRORISM TOGETHER

VIGILANCE, PREVENTION,
AND PROTECTION AGAINST
THE TERRORIST THREAT

December 2016 edition

VIGIPIRATE



**« We are a free people.
We do not yield to any pressure,
and we are not afraid,
because we carry an ideal
that is greater than us
and that we are capable
of defending wherever peace
is threatened. »**

Address by the President of France
to the Nation following the events
of 7 and 8 January 2015 –
9 January 2015

PREFACE

Since 7 January 2015, a wave of attacks of particularly dramatic intensity has been unleashed against our country. Unfortunately, using such methods of spreading intimidation and horror is not something new in our history. Nonetheless, there is a need to note a change of scale and of nature in the terrorist violence that we face. The brutality of the means used attests to the will (which, as it happens, has been made clear) to indulge in mass killing in an indiscriminate manner. Moreover, the profiles of the perpetrators of those acts confirm a double threat, one that is projected from abroad and nourished from within via propaganda from terrorist organisations that seek to turn our fellow citizens against their own country.

To counter that terrorist risk, France is taking firm, resolute action. While our country continues to be fully involved abroad, both diplomatically and militarily, our internal security arrangements have been considerably hardened. Legally, institutionally, and financially, a considerable effort has been made to increase and improve the means at our disposal, in order to strengthen the co-ordination of our riposte and to ascertain the full set of factors that feed the phenomenon of radicalisation.

At the heart of that response made by the public authorities, the VIGIPIRATE plan occupies a special place. Set up in 1978, and triggered for the first time in 1991 during the Gulf War, the plan is an essential instrument of vigilance, prevention, and protection against the terrorist threat. Designed for all state actors, it offers them operational measures and a mobilising framework to enable them to anticipate and respond to that threat. Based on its approximately 300 measures, some of which are additional and, thus, only triggered when needed, it constitutes a complete tool that can be fine-tuned to meet circumstances.

To further consolidate that instrument and adapt it to changes in the threat, rewriting the VIGIPIRATE Plan nonetheless became a necessity. That was done with the ambition of widely disseminating a culture of security amongst our fellow citizens. In its new approach, the plan intends to better inform each one of us on terrorism, the mechanisms deployed to deal with it, and the actions and behaviour that protect and save. Faced with a diffuse, polymorphic threat, the State's duty of protection must not lead to citizens becoming disengaged. On the contrary, each person must make an individual commitment to collective security, because each person is responsible for everyone.

Make a contribution to mobilising the Nation against terrorism: that is the ambition of this new plan, which is supported by the Secretariat General for Defence and National Security.

Louis Gautier
Secretary General
for Defence
and National Security



CONTENTS

▶ Preface	3
▶ Introduction	6
▶ Part 1. The VIGIPIRATE plan	11
1. Principles and objectives	12
1.1. A government plan for vigilance, prevention, and protection	12
1.2. One plan, many actors	14
2. The various actors of national security	16
2.1. The State	16
2.2. Local authorities	16
2.3. Businesses	17
2.4. The citizenry	17
2.5. Actors abroad	17
3. A security arrangement that is under permanent adaptation	18
3.1. Assessing the threat	18
3.2. Knowing the vulnerabilities of targets in order to reduce them	18
3.3. Adapting the VIGIPIRATE stance	19
▶ Partie 2. Tous impliqués	23
1. Getting ready	24
1.1. As a citizen, what can I do?	24
1.2. Directors and heads of sites that deal with the public, how can you get ready?	25
2. Prevention	34
2.1. Preventing and flagging up cases of radicalisation	34
2.2. Preventing the move to take violent action, and flagging up suspicious situations	36
3. Reaction	42
3.1. What can be done in the event of an armed attack?	42
3.2. What can be done in the event of a cyberattack?	47
3.3. What can be done in the event of an attack using a toxic product?	48
4. Managing the post-attack situation	50
4.1. If you have witnessed a terrorist attack	50
4.2. If you have been the victim of a terrorist attack	50

▶ Part 3. Areas of action	53
1. Alerting and mobilising	54
2. Protecting mass meetings	55
3. Protecting installations and buildings.	56
4. Protecting dangerous installations and materials	57
5. Ensuring cybersecurity	58
6. Protecting the air sector	59
7. Protecting the maritime sector.	60
8. Protecting land transport	61
9. Protecting the health sector.	62
10. Protecting the food chain	63
11. Protecting networks (communications, water, electricity, hydrocarbons, gas)	64
12. Controlling borders	68
13. Protecting French nationals and interests abroad	69
▶ For more information.	70
▶ Glossary	72
▶ Useful numbers	74

INTRODUCTION

The VIGIPIRATE plan is at the heart of the national arrangement for protection against the terrorist threat

In the first line of threats identified in the national security strategy¹ there appears the terrorist threat, regardless of whether it is applied on national territory, against our nationals and interests abroad, or in cyberspace. To face up to it, France has a complete national arrangement that includes the VIGIPIRATE plan.

This decision-making support tool is provided to the Prime Minister. It brings together all national actors (the State, local authorities, public and private operators, and citizens) in an initiative that combines **vigilance**, **prevention**, and **protection**.

VIGIPIRATE: a national plan and global security arrangement

The State must be able to react and to take necessary measures in the event of a threat being made against the population or against the regular functioning of the country's institutional, economic, or social life.

To that end, **the State has a set of plans**. Those planning documents are developed at local or national level in preparation for wide-ranging crises and catastrophes.

Around twenty plans are in existence, and there are the same number of specific variants. They are divided into two broad categories: **national plans and territorial plans**.

Drawn up under the ægis of the Secrétariat général de la défense et de la sécurité nationale (SGDSN – Secretariat General for Defence and National Security), **national plans are decision-making support tools for the highest authorities of the State**. In the event of a major crisis, they **facilitate the co-ordination of all the actors concerned**, in the first line of which stand the various ministries.

VIGIPIRATE is the only national plan that is permanently implemented. Thus, VIGIPIRATE is a planning document as well as a national security arrangement that is in constant development.

1- Introduced in 2008 by the White Paper on defence and national security. See the "For more information" section, page 70.

Faced with the terrorist threat, a set of complementary plans, the **PIRATE family plans**, was drawn up. **Of those anti-terrorist plans, VIGIPIRATE is the only one to be permanently active**, because it implements a vast arrangement for vigilance, prevention, and protection that involves a very large number of actors: ministries, internal security forces, public and private operators, and the citizenry.

The other PIRATE family plans are intervention plans. Their purpose is to be activated in the event of a terrorist attack, in a specific context, such as the air or maritime environment or cyberspace; those are the NRBC, PIRATAIR-INTRUSAIR, PIRATE-MER, PIRANET, and METROPIRATE plans².

Architecture and functioning of the VIGIPIRATE plan

The VIGIPIRATE plan includes **300 measures that apply to 13 wide areas of action, such as transport, health, and networks (detailed in part 3)**. Those measures are spread out between a core of permanent measures and a set of additional measures. Those measures can be activated based on the development of the threat and vulnerabilities.

Based on the terrorist-threat assessment made by the intelligence services, **the SGDSN circulates interministerial directives** (the “VIGIPIRATE stance memos”) **that determine the measures that must be implemented** by the actors concerned by vigilance, prevention, and protection in the face of terrorist-action threats.

Those stances are circulated:

- ⦿ at certain specific periods of the year: the start of the academic year, the end-of-year holidays, etc.;
- ⦿ as part of large national events: the celebrations marking the 70th anniversary of the Normandy landings, Euro 2016, COP21;
- ⦿ following an attack in France or abroad, in order to urgently adapt the national protection arrangement.

The initiative is based on three main principles:

- ⦿ **a cross-analysis of the threat and vulnerabilities;**
- ⦿ **organisation by area of action**, identifying the levers that enable a reduction in the vulnerabilities of the large sectors of the country based on the intensity of the threat;
- ⦿ an **approach based on security objectives** that enables the most suitable measures to be selected, together with their application procedures.

300
mesures
13
areas
of action

2- See the “For further information” section, page 70.

The terrorist threat remains at a high level on a persistent basis

Terrorism

In its 2013 White Paper on defence and national security, France defines terrorism as “a mode of action used by adversaries that do not abide by the rules of conventional warfare.” Terrorism is complex; “[it strikes] civilians indiscriminately, and the violence [that it uses] aims first at taking advantage of the effects that its brutal irruption produces on public opinion in order to constrain governments.”

Defined as such, terrorism is widespread around the world and comes in many forms. Its constant development makes it particularly difficult to grasp.

Today, a phenomenon that is mainly Jihadist-inspired

Terrorism is **a phenomenon with a very long history, and it can be linked to arrange of claims**. Over the last few decades, organisations making nationalist claims or linked to decolonisation, as well as groups upholding extremist ideologies with a political or religious basis, have committed attacks on national territory.

The 1995 attacks in France revealed the terrorist nature of the Jihadist threat, which moved onto the world stage on 11 September 2001. Taken to an unprecedented level around the world, it is embodied in particular by Al Qaida, Daesh, and their affiliated networks, whose **plan is to use violence to impose an Islamist ideology**. Since 2015, the terrorist threat has persisted at a very high level in Europe, especially in France.

The terrorist threat in France

French nationals and French interests being exposed to the terrorist threat, on national territory or abroad, is explained in particular by the values and lifestyle promoted by the French Republic.

The attacks that hit France in 2015 and 2016 showed us the need to incorporate that phenomenon into our daily life.

Three major characteristics of that development should be highlighted:

- ① the **multiplication of the types of actors** (isolated radicalised persons, operational teams deployed in Europe);
- ② the **diversification of operating methods** (opportunistic attacks, planned attacks);
- ③ the **multiplication of targets** (infrastructures, gatherings, symbolic places, etc.).

Terrorist attacks can also induce knock-on and imitation effects. Some individuals with extreme ideas seeking social revenge or identity claims, or who sometimes suffer from psychological disorders, can be encouraged to take action.

Operating methods used by terrorists

With the aim of hitting France or its interests, terrorists use a wide range of means and different operating methods, based on their level of preparation.

Possible operating methods³:

- **mass shootings** (with the possible use of explosive charges);
- **the follow-up attack following an initial attack**, in order to strike rescuers, the police, or the *gendarmerie* at the scene;
- **the assassination of public figures** (political, religious, representative of the security forces, military personnel, etc.);
- **the use of booby-trapped cars, parcels, or letters**;
- **the use of toxic chemicals**;
- **the destruction of symbolic infrastructures**;
- **wide-ranging cyberattacks**, taking account of the developments of information technology and of digital technology in daily life;
- **hostage-taking**;
- **multiplying false bomb alerts**, or announcing fake attacks, with the aim of establishing a climate of fear.

The types of weapons used:

Terrorists use a vast range of weapons, ranging from knives to explosive devices and including targeted weapons (ram-vehicles, etc.).

3- This list is not exhaustive, because terrorist operating methods constantly change and adapt, and they can be combined.



▶ PART 1

THE VIGIPIRATE PLAN

1. PRINCIPLES AND OBJECTIVES

1.1. A government plan for vigilance, prevention, and protection

The VIGIPIRATE plan rests on three pillars:

1. **vigilance** is linked to knowledge of the terrorist threat and to its due recognition, in order to adjust the behaviour of each individual and the protection measures;
2. **prevention** is based on raising awareness of the terrorist threat amongst State agents, operators, and citizens, on their knowledge of the organisation of the national arrangement, and on the good preparation of means of protection and response; and, finally,
3. **protection** is based on a wide range of measures that must be constantly adaptable to the situation in order to reduce vulnerabilities without inducing disproportionate constraints on the economic and social life of the Nation.



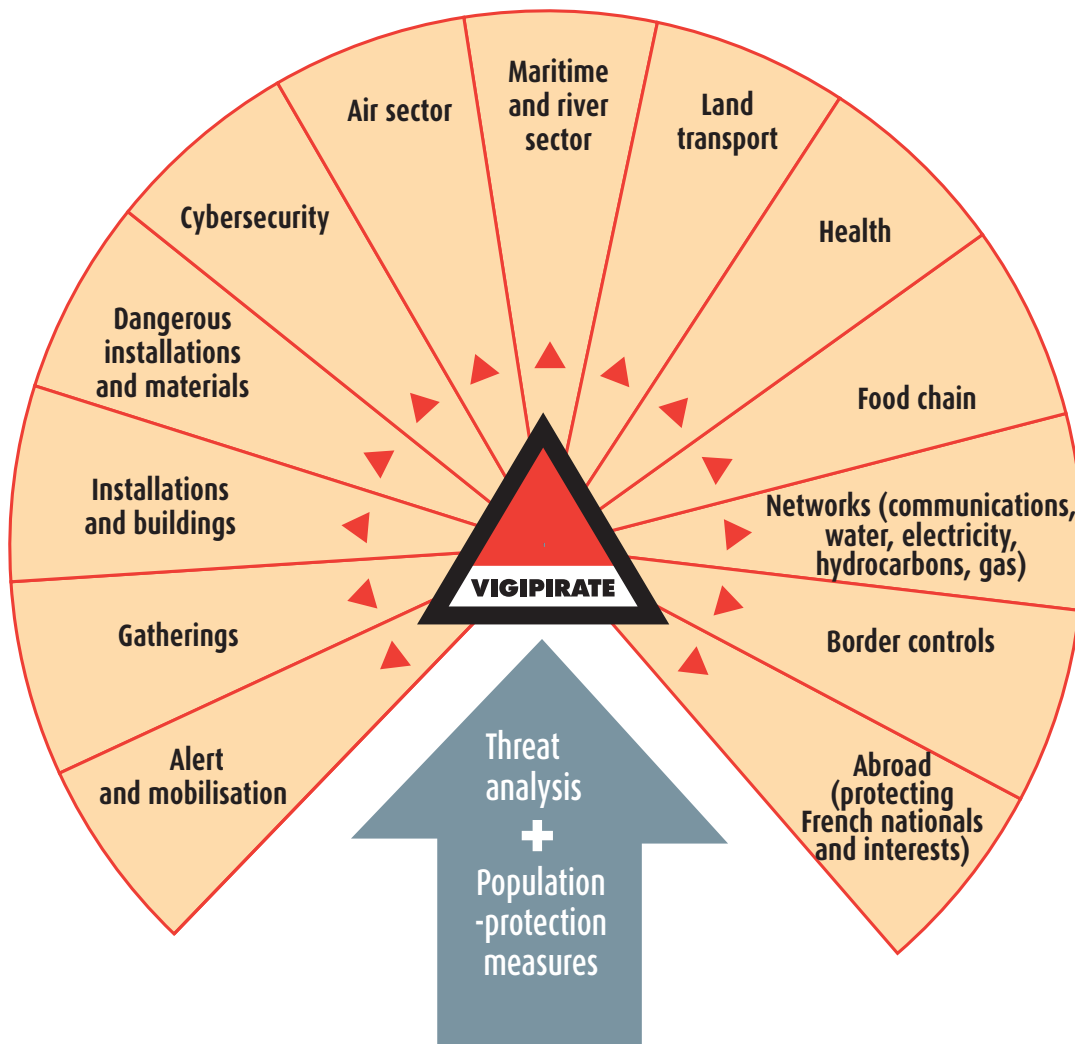
Vigilance
Prevention
Protection

The plan defines **thirteen areas of action**, i.e. twelve areas covering national territory and one area covering matters abroad. An area of action is made up of an activity sector or a family of potential targets. The various areas of action contain descriptions of:

- **characteristics, challenges, and actors;**
- **security objectives** specific to the sector;
- **permanent vigilance and protection measures** to be implemented in all circumstances, and that form the permanent basis for vigilance, prevention, and protection;
- **additional measures** that are likely to be implemented on the basis of the assessment of the terrorist threat or during periods of particular vulnerability.

Where permanent or additional, measures can be recommendations or they can be compulsory, as provided for in law.

The VIGIPIRATE plan's 13 areas of action



In some areas, the VIGIPIRATE plan is supplemented by specific intervention plans that implement specialist means (the NRBC, PIRATAIR-INTRUSAIR, PIRATE-MER, PIRANET, and METROPIRATE plans).

1.2. One plan, many actors

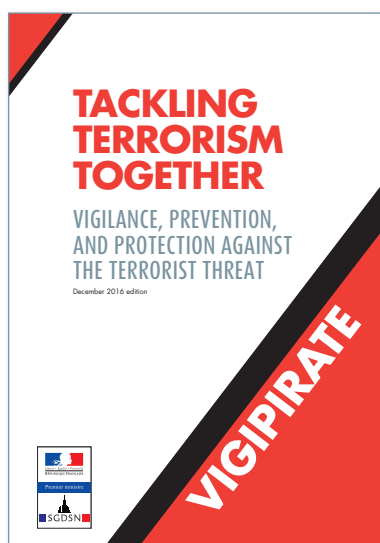
The VIGIPIRATE plan is made up of a set of documents aimed at various actors. It comes in two parts, a public part and a “confidential defence” classified part.

A **public document** (this document) enables public and private businesses, local authorities, and each citizen to understand the functioning of the VIGIPIRATE plan. **An educational tool and accessible to all**, the public part of the plan contributes to **developing a culture of collective security**.

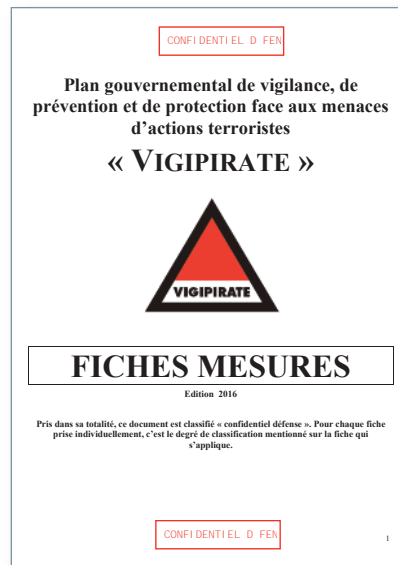
Some information and the plan’s implementation procedures must be protected, so they are classified, in particular to stop potential adversaries from exploiting them. The “confidential defence” part of the VIGIPIRATE plan includes two documents:

- ① the plan itself, which details strategy, objectives, and measures for all areas of action;
- ② an annexe made up of all of the measures sheets. The latter are emergency instructions that aim at helping the operational implementation of measures, and specifying their legal framework of application.

A public part: a document presenting the VIGIPIRATE plan and setting out advice for behaviour, aimed at the citizenry and at security professionals



A “confidential defence” part:
the full plan, aimed at State institutions
and some private operators



2. THE VARIOUS ACTORS OF NATIONAL SECURITY

The VIGIPIRATE plan is a tool to mobilise the whole Nation in the face of the terrorist threat. With the State at the centre, it gathers up the various categories of actors who represent potential targets for terrorists.

2.1. The State

The **Prime Minister** decides on the implementation of the provisions and measures set out in the VIGIPIRATE government plan. The SGDSN, which is attached directly to the Prime Minister, steers the VIGIPIRATE plan.

The **Minister of the Interior**, who is responsible for internal security, public order, protecting people, and safeguarding installations and resources of general interest, oversees the proper operational execution of the measures activated or implemented across the whole territory.

The **Minister of Foreign Affairs and International Development** oversees the implementation of specific measures when the threat is aimed at French nationals, representations, assets, or interests abroad.

The **Minister of Defence** engages the armed forces in land, sea, air, and cyberenvironments, as part of the government's overall manoeuvre to fight terrorism on national territory.

Each minister implements the appropriate instructions and measures in the directorates, establishments, central departments, and decentralised departments, and passes them on to operators of vital importance, public services, large businesses, and professional bodies that intervene in the minister's areas of competence.

At local level, the **département prefects** (under the co-ordination of the prefects of defence and security areas) ensure that information is given to various public and private actors. In addition, they ensure consistency in implementing measures in territories in compliance with their respective competences and responsibilities.

2.2. Local authorities

Local authorities exercise responsibilities in several sectors of the economic and social life of the Nation. The implementation of the VIGIPIRATE plan concerns them in several ways:

- **protecting their installations, infrastructures, and networks;**
- the **continuity of public services** for which they are responsible;
- **protecting their agents;**
- the **security of cultural, sports, or festive gatherings** that they organise or host.

In that way, local authorities, in liaison with the prefect, enable **continuity of the general arrangement** for vigilance, prevention, and de protection.

2.3. Businesses

Certain businesses are designated “Opérateurs d’Importance Vitale”⁴ (OIV – Operators of Vital Importance). They are legally required to implement specific protection measures contained in regulations relating to the security of activities of vital importance and in the VIGIPIRATE plan.

Generally speaking, all public and private businesses must ensure their own security and, where appropriate, the security of people whom they host. They implement measures adopted subject to the prerogatives they are granted by law.

2.4. The citizenry

Responsible behaviour by all citizens contributes to vigilance and to prevention, as well as to protecting the community against terrorist threats. The VIGIPIRATE public plan familiarises citizens with the behaviour to be adopted in the event of a terrorist threat.

2.5. Actors abroad

The security of all French nationals abroad is, **in the first instance, the responsibility of their host State**. Nonetheless, all operators and **all businesses are required to ensure the security of their employees**.

The Ministry of Foreign Affairs and International Development passes on its instructions to all diplomatic missions, which in turn pass those instructions on to the French community, employers, local media, and host States.

4- See the “Glossary” section, page 73..

3. A SECURITY ARRANGEMENT THAT IS UNDER PERMANENT ADAPTATION

The VIGIPIRATE plan enables permanent adaptation of the vigilance, prevention, and protection arrangement in the face of threats of terrorist action. To that end, directives called “VIGIPIRATE stances” are regularly circulated by the entire ministerial and prefectural chain.

Those stances are prepared by the SGDSN in close co-ordination with the departments of all ministries. They are circulated at certain specific times of year (the start of the academic year, the end-of year holidays, the summer period, etc.), as part of preparations for large national events (the 70th anniversary of the Normandy landings in 2014, COP21 in 2016, Euro 2016, etc.), or after an attack.

Implementing the VIGIPIRATE plan combines three approaches:

1. **assessing the terrorist threat** in France and against French nationals and interests abroad;
2. **knowing the vulnerabilities of potential targets** of a terrorist attack, in order to reduce them and to take preventive action to limit the effects of such an attack;
3. **determining a security arrangement** that responds to the level of risk arising from the crossover between the vulnerabilities with the state of the threat.

3.1. Assessing the threat

The assessment of the terrorist threat is made by a specific working group that brings together all the intelligence services, mandated and facilitated by the national intelligence co-ordinator.

It provides a regular assessment based on current events. That assessment can be supplemented by thematic assessments, applied to sectors, areas of activity, or subjects of particular interest.

These analyses are used to prepare VIGIPIRATE stance memos.

3.2. Knowing the vulnerabilities of targets in order to reduce them

The plan defines **thirteen areas of action**⁵, twelve covering national territory and one covering matters abroad. An area of action is made up of a sector of activity or a family of potential targets, which allows a consistent response strategy to be defined.

Hence, in relation to each area of action, a description is given of a strategy that details the vulnerabilities of the setting concerned, and defines the security objectives to be implemented to reduce their weaknesses in the face of the threat.

⁵- See the list of areas, page 13, as well as part 3, “Areas of action”.

Each security objective is based on operational measures that are ranked by the degree of constraint involved in implementing them. Two types of measures are distinguished:

- ① **permanent measures** (or **base measures**), which constitute the permanent security stance;
- ② **additional measures**, of which some can be very constricting, and which are implemented on a case-by-case basis as well as being limited in time, to face up to the worsening of the threat and / or vulnerabilities.

Some measures, whether permanent or additional, are compulsory.

Other measures come under best practice in security matters, of which the implementation is recommended by the VIGIPIRATE plan. They are the subject of adapted communication that aims at encouraging the actors concerned to apply them.

Most measures are placed in the public domain for ease of circulation. Only a few additional measures are confidential, because their publication may facilitate terrorist action.

The conditions for implementing measures (especially in the legal domain) are detailed in implementation-support sheets called measures sheets, which are attached to the “confidential defence” plan.

3.3. Adapting the VIGIPIRATE stance

The VIGIPIRATE stance is an interministerial directive determined by the Prime Minister; it adapts the vigilance, prevention, and protection arrangement. It **includes the VIGIPIRATE level, the security objectives selected, active measures, and government communication items**. It specifies base measures and mentions the additional measures decided upon, with, where appropriate, details of their context and their application procedures, as well as the duration for which they are implemented.

It is set out in a confidential document that also contains the assessment of the terrorist threat. It is validated by the Prime Minister and circulated by the SGDSN. The stance is applied by each ministry through specific directives.

3.3.1. The VIGIPIRATE level




The VIGIPIRATE level is made public. It is aimed at **indicating the vigilance of the Nation in the face of the terrorist threat, and, if needed, putting the country on alert** in the face of a situation involving a verified threat or an attack that has been carried out. It covers only national territory and the DOM-COM (*Départements et Collectivités d’Outre-Mer – Overseas Départements and Authorities*).

It is determined by the Prime Minister following the assessment of the terrorist threat made by the crossover between the threat and vulnerabilities.

The arrangement chosen must be strictly dimensioned in line with the assessment of the threat.

Three levels are distinguished:

“vigilance”, “reinforced security – attack risk”, and “attack emergency”.

Levels	Level-activation principles	Implementation conditions	Types of measures activated
Vigilance 	<p>This level relates to the permanent security stance</p>	<p>This level is valid everywhere and at all times.</p>	<p>Implementation of all permanent measures (base).</p>
Reinforced security - threat risk 	<p>This level expresses the State's response to a heightened level of terrorist threat.</p>	<p>This level can apply to the whole of national territory, or it can be targeted on a geographical area or a particular sector of activity. This level does not have a set time limit.</p>	<p>Reinforcement of permanent measures and activation of additional measures.</p>
Attack emergency 	<p>This level triggers a maximum state of vigilance and protection, either in the event of a documented and imminent terrorist attack threat⁶, or immediately after an attack.</p> <p>Activating this level enables the protection arrangement to be adapted to prevent any risk of a follow-up attack.</p>	<p>This level can be activated across the whole of national territory, or across a defined geographical area.</p> <p>The "attack emergency" level is of short duration, and can be deactivated at the end of crisis management.</p>	<p>Permanent measures reinforced and additional measures activated.</p> <p>This level is associated with constricting additional measures, and with a reinforcement of the alert that can be coupled with information being circulated using the SAIP⁷ telephone application, the various institutional web sites, and radio. Behavioural advice can also be circulated to the population in case of the risk of a follow-up attack.</p>

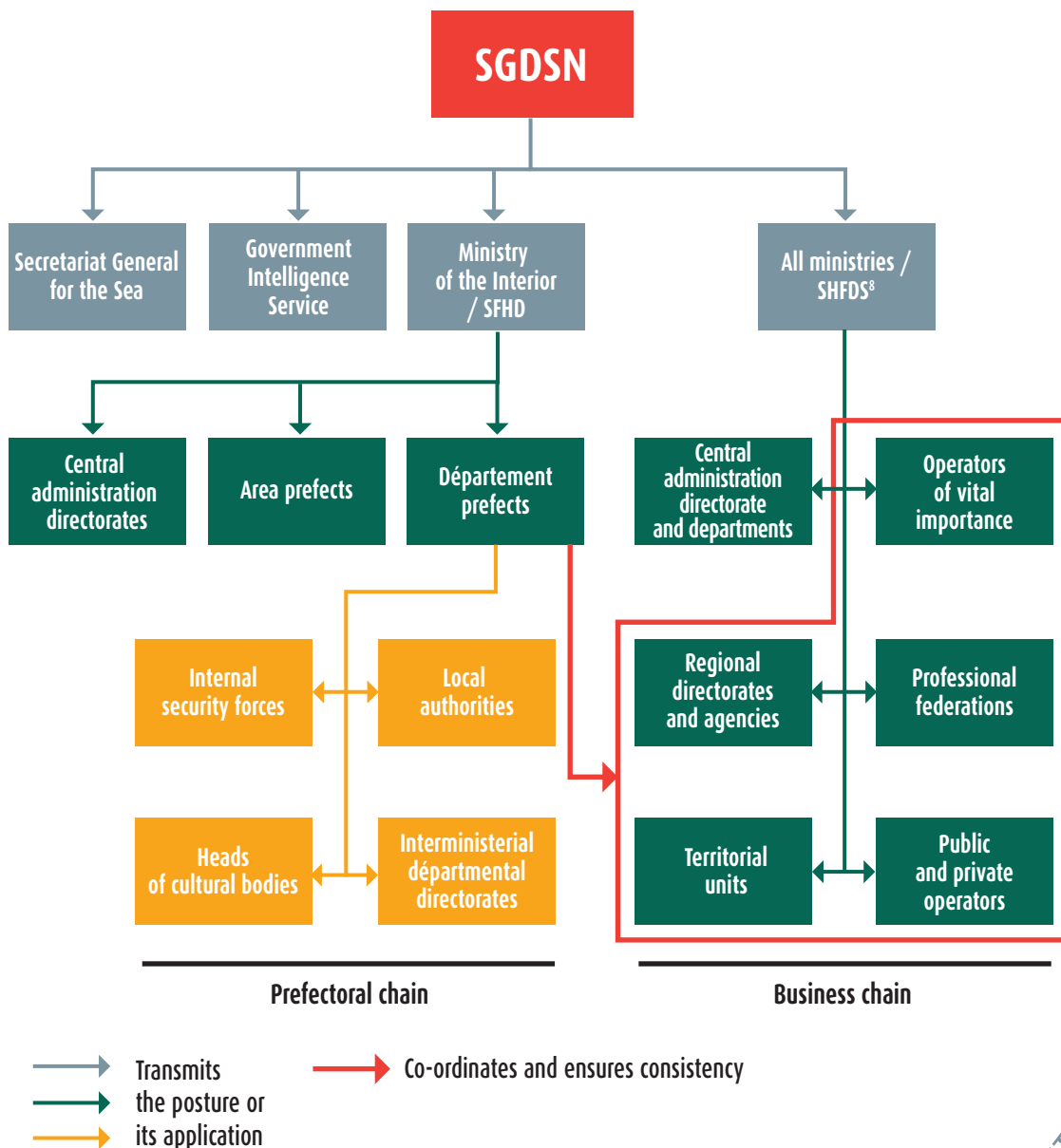
6- The definition of the imminence remains subjective. Objectivity, on the basis of information issued by the intelligence community, involves giving precise answers to at least two of the following four questions: who? where? when? and how?

7- SAIP: *Système d'alerte et d'information des populations* (Population Alert and Information System, a smartphone application). See "For further information", page 71, and "Glossary", page 73

3.3.2. Circulating VIGIPIRATE stance instructions

In accordance with instructions given by the Prime Minister, each ministry gives instructions within its own field of competence. The Ministry of the Interior plays a leading role in national territory through prefects, the national police, the national *gendarmerie*, and civil security. Measures are implemented by a wide variety of actors: State actors (administrations, decentralised departments), local authorities, public and private businesses, professional federations, etc. Citizens are also called upon to be actors in certain simple vigilance measures.

Circulation circuit of VIGIPIRATE stance memos and instructions



8- SHFDS: *Service du haut fonctionnaire de défense et de sécurité* (Department of the Senior Officer of Defence and Security).



▶ PART 2

EVERYONE IS INVOLVED

1. GETTING READY

1.1. As a citizen, what can I do?

1.1.1. Why should you be an attentive citizen?

Most of the time, terrorists act with a political, identity, or ideological objective. To reach it, they seek to break the unity of societies that they attack by breaking the fundamental links that make up those societies.

Concern over security must lead us to reinforce our collective vigilance, but we must not be wary of everyone. The true resilience of the Nation rests on all citizens adhering to common values and not to evicting a few people.

Being attentive means:

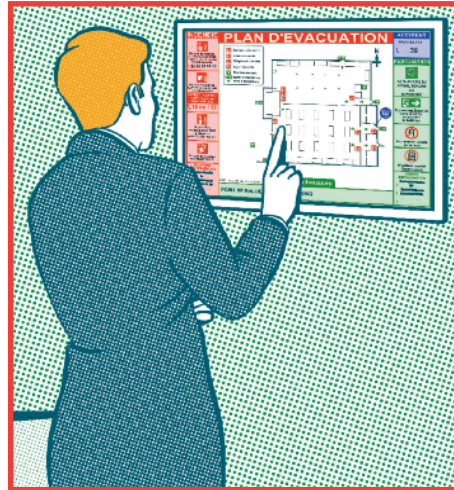
- ① maintaining an open rather than a fearful view of others;
- ① acting for the security of all by flagging up any risky situation or behaviour;
- ① prevent any individuals from tipping over into criminal behaviour by flagging them up, out of a concern for protecting the population and for protecting those individuals from themselves;
- ① ensuring that our own behaviour does not endanger the security of others (false rumours, etc.), and that it does not nurture a climate of fear.

Be attentive
to others
and to one's
environment

1.1.2. How can I be an attentive citizen?

Get to know your daily environment well:

- ◉ get to know the configuration of the living areas and of the sites that you usually frequent: building, street, neighbourhood, building layouts, development of spaces, emergency routes and exits;
- ◉ get to know to whom you must report unusual behaviour and situations;
- ◉ get into the habit of observing your environment carefully, especially when you are in areas of heavy traffic (stations, public transport, large gatherings, etc.).



Get ready and anticipate emergency situations:

- ◉ rely on your intuition;
- ◉ get ready to experience a potentially violent situation:
 - for each place in which you find yourself, think of the most appropriate reaction in case of attack;
 - identify emergency exits;
 - establish an evacuation route from all enclosed places or places where large gatherings are held (cinemas, swimming pools, shopping centres, etc.);
- ◉ always have emergency numbers with you;
- ◉ download the SAIP application to your smartphone⁹.

Always behave responsibly:

- ◉ ensure that your attitude or your behaviour do not make people think that you may have malicious intent (masking your face by wearing a motorcycle helmet within a public building, using fake weapons or disguising yourself in paramilitary clothing along public roads, false bomb alerts, verbal threats of a terrorist nature, etc.);
- ◉ do not take photos near sites where photography is prohibited;
- ◉ comply with recommendations and instructions from public authorities, law-enforcement agencies, and security officials (inspecting bags, packets, hand luggage, security pat-downs, complying with security parameters);
- ◉ do not point out the control devices put in place by law-enforcement agencies (high-beam flashes along the road to signal a roadblock, etc.);
- ◉ do not pass on false rumours;
- ◉ do not leave personal effects (bags, luggage) unattended;
- ◉ when travelling, do not agree to take responsibility for an item of luggage, an object, or a package from someone you do not know.

⁹- See "For further information", page 71.

Get first-aid training:

- alerting the emergency services, performing a cardiac massage, and treating h emorrhages are essential procedures that can be carried out during situations of exceptional seriousness. Those essential procedures can save lives;
- several accredited civil-security associations teach first aid and provide first-aid training. Accreditation is granted after the associations' competences have been verified;
- if you wish to receive first-aid training, see the list of associations accredited for first-aid training¹⁰.

**Preparing for journeys abroad:**

Before each journey abroad:

- check <http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs> for advice that is updated regularly;
- make an entry for your journey on the Ariane portal, <https://pastel.diplomatie.gouv.fr/fildariane/dyn/protected/accueil/formAccueil.html>, to receive any alerts;
- if going abroad on a long-term basis (i.e. for more than 6 months), French nationals and their families must have themselves entered in the register of French nationals living abroad, and do so at the competent French consulate.

1.1.3. Cybervigilance**Acquire good internet habits:**

The lives of businesses, administrations, and our fellow citizens are henceforth dependant on digital technology and ICT resources on a daily basis. Those tools can form a powerful vector for terrorists who want to attack society as a whole. For that reason, it is essential to protect yourself by acquiring good habits:

- protect your personal, and professional information as well as your digital identity;
- always be careful when you click on links and attachments;
- choose passwords composed for each account;
- keep your passwords secret, and never reveal them to anyone;
- never reveal your payment-card number by e-mail;
- make your payments using secure sites;
- protect your data when travelling;
- give preference to secure WiFi access and personal removable supports (USB sticks);
- regularly update the software installed on your computers, smartphones, and tablets, especially your antivirus software;
- deactivate wireless interfaces when they are not necessary;

¹⁰- See the list of accredited associations at <http://www.gouvernement.fr/risques/se-former-aux-premiers-secours>

- make regular back-ups;
- consider making your internet box secure;
- flag up suspicious web sites and social networks, or those that advocate terrorism¹¹.

You will find recommendations and best practices at the ANSSI website:

- for administrations: <http://ssi.gouv.fr/administration/bonnes-pratiques>
- for businesses: <http://ssi.gouv.fr/entreprise/precautions-elementaires>
- for individuals: <http://ssi.gouv.fr/particulier/precautions-elementaires>
- for everyone: le site <http://www.risques.gouv.fr>



Knowing how to protect your identity and your personal information:

The internet offers many opportunities for sharing moments from your private life. The increase in social networks enables you to keep in touch with your family and friends, but those networks are not risk-free for your security. Moreover, when you use them, keep in mind that an ill-intentioned person may make criminal use of the information that you publish.

When you work in a profession that may be a terrorist target, **it is strongly recommended that you do not divulge information about where you live and about your habits**, that you always think of the use that can be made of your details, and that you preserve the confidentiality of your private life as much as possible.

Your digital identity is precious, and the traces that you leave by publishing your personal information will remain accessible almost indefinitely.

Terrorists use data on the internet to get to know their targets better and to reach them better

Consequently, protect yourself and those close to you by being careful about what you publish on the internet.

11- Report matters at <https://www.internet-signalement.gouv.fr/>

1.2. Directors and heads of sites that welcome the public, how can you get ready?

All heads of establishments that deal with the public are encouraged to apply the VIGIPIRATE plan as part of their own business security plan. This plan sets out the measures to be taken in the event of a threat or an attack, or in the case of risks like discovering abandoned objects.

It sets out the special arrangements to be applied in matters of surveillance, organisation, and control. Individual company officials are informed of what they must do as part of the business plan.

The State particularly encourages establishments that deal with the public to **establish reaction procedures in the event of a terrorist attack, and to raise awareness amongst their employees.**

To that end, the authorities, in liaison with the actors concerned, have prepared a set of **guides to best practices**¹² aimed at the heads of establishments that deal with the public, which set out the individual and collective behaviour to be followed to prepare for a terrorist attack.

Good prior organisation of your establishments and adapted reactions from staff can save lives.

1.2.1. Preparing your organisation for a malicious or terrorist act

Several pieces of advice are set out below. Some would be difficult to apply by all sites, so they must be adapted to the situation.

a) Developing relationships with external partners

The various external partners:

- ① **prefects and prefectural departments.** They assess the threat level and establish the vigilance and protection measures to be adopted as part of implementing the VIGIPIRATE plan;
- ① **mayors and municipal departments.** They supplement action taken by the police and the *gendarmerie*. Along public roads, they carry out development work that is needed for protecting exposed installations;
- ① **the police and the *gendarmerie*.** They can use their security references to provide security advice to heads of sites with respect to reinforcing their security measures. Regular meetings with the police and the *gendarmerie* are part of mutual knowledge. For sites that are particularly sensitive, building plans can be passed to the security forces in order to facilitate an intervention in the event of an attack.

¹²- See the sector guides to best practices at <http://www.gouvernement.fr/reagir-attaque-terroriste>

b) Analyse your establishment's vulnerabilities

- ⊙ identify what makes your establishment a target (a site for large gatherings of people, a site representing the country's institutions, a site symbolising the Western way of life or the values of the French Republic, a place of worship, etc.);
- ⊙ identify what could be targeted in your establishment: staff, infrastructures, specific equipment, information or products that could be stolen with a view to terrorist action;
- ⊙ identify the establishment's physical vulnerabilities (number of access points, doors that do not lock, unsupervised delivery access points, etc.);
- ⊙ consider possible means of action (cold weapons, automatic weapons, ram-vehicles, booby-trapped parcel or vehicle);
- ⊙ take account of the internal threat (for example, radicalisation that can turn violent).

c) Get organised

Reinforce site protection:

- ⊙ limit the number of access points for better flow surveillance, without reducing evacuation capacity for your employees and for the public;
- ⊙ deploy a video-protection system;
- ⊙ put in place a system of access badges;
- ⊙ install an interphone system with a camera if possible;
- ⊙ ensure that there is lighting at access doors to the site;
- ⊙ regularly change the codes of Digicode-type alphanumeric keyboards / keypads;
- ⊙ put in place a filtering and search system at access points;
- ⊙ protect the site's external access points against all chances of a ram-vehicle attack (installing studs, flowerboxes, concrete blocks, mobile portcullises, etc.);
- ⊙ ensure that there is co-ordination between you and surrounding establishments or businesses;
- ⊙ ensure that the site's communal areas and technical areas are kept clean, and that abandoned parcels cannot be hidden there;
- ⊙ check the availability of emergency exits.

Put in place specific means of alert:

- ⊙ **Alert within the organisation.** It is essential that each organisation is able to sound the alert in the event of a terrorist attack. The alert system governs the reaction of all persons occupying the site, and must be different from the fire alarm, because the expected reaction is not the same. Such a system cannot be improvised, and it is recommended that the system be set up in consultation with the staff of the establishment. Everyone must know those means of alert, which must be tested regularly during drills and exercises.
- ⊙ For the alert procedure to be complete, two systems must be put in place:
 - a **decentralised alert system** that enables each person to sound the alert once the malicious act has been noted (whistle, landline, telephone text message, beeper system, radio, etc.);
 - a **centralised alert system** that allows a warning to be given to the whole site (especially if it is extensive): an audible alarm that is different from the fire alarm, a message broadcast by loudspeaker, a warning light, telephone text message, foghorn, etc.

- **The aim of the alert is to prevent an attack.** Ideally, two types of attack must be distinguished, because they do not call for the same reactions:
 - an external attack against the site or close to it (containment recommended);
 - an attack at the site (evacuation or containment, based on the location of persons in the building). **In the event of an internal attack, it is not recommended that a single reaction be used for the whole of the site concerned.** Some people may be able to escape easily given the location of their premises, others may not be able to escape easily and must, therefore, place themselves in containment. Consequently, it is preferable to leave the initiative to persons occupying the site.

Different audible or visual codes can be used to distinguish the two types of attack (internal and external). For example, an external attack can be indicated by 3 long ringing tones, whilst an attack on at the site can be indicated by 6 long ringing tones. Similarly, if the alert is sounded by text message, the message must specify if the attack is internal or external to the site.

- **Send an alert outside the organisation:** security forces, sensitive external establishments (hospitals, schools, etc.). **The sooner the alert is given, the sooner internal security forces can intervene.**
- Make your employees aware of the fact that each one must feel responsible and must give a warning in the event of an attack. The message to be sent out is as follows: **“Don’t think that others have sounded the alert. Do it yourself.”**

Be prepared:

- a **crisis kit** with the telephone numbers of persons to be contacted and the plans of the site that can be given to security forces in case of an attack;
- **reaction procedures adapted** to various malicious acts:
 - bomb alert (give preference to the same reaction as a fire alert);
 - an attack within the site (evacuation or containment);
 - an external attack that is close to the site (prefer containment);
- **evacuation itineraries** (which are not necessarily emergency exits – for example, a roof may offer protection);
- **containment rooms** that are known to everyone. Door closures can be reinforced at low cost.

Raise awareness amongst staff:

Inform staff:

- inform officials of the threat and of the various best practices to be followed in the event of a terrorist threat;
- develop an internal awareness-raising strategy by displaying the poster (see page 43) and by showing the video entitled (How to react in the event of a terrorist attack”¹³. Guides to best practices that are specific to certain professional sectors can also be distributed;
- make staff aware of complying with security and vigilance measures;
- give reminders of procedures and of each person’s role:
 - inform officials of the procedure for flagging up suspicious behaviour (employees who show signs of holding extreme and potentially violent thoughts);
 - encourage employee vigilance in order to detect and flag up suspicious behaviour.



Train staff:

- encourage first-aid training;
- ensure that everyone knows about means of alert and how to use them;
- encourage site knowledge by organising “exploratory reconnaissance missions” in order to identify routes, emergency exits, possible obstacles, and anything that may offer protection;
- organise simple drills and collective exercises that may possibly incorporate the various partners, and by systematically exploiting feedback from those exercises.

1.2.2. Prepare for a gathering¹⁴

Event security cannot be improvised. Seek advice from professionals. To prepare for a gathering of people, you must:

a) Identify threats and vulnerabilities

Assess the sensitivity of the gathering in conjunction with the State’s services. Why may terrorists target the gathering? In what way is it a symbol of the Western way of life and of the values of the Republic? Does the gathering have media coverage that may give a high level of visibility to terrorist action?

Consider the various possible attacks: throwing or depositing an explosive device, a booby-trapped vehicle parked on the approaches to the site, a ram-vehicle, shooting, a cold-weapon attack, etc.

Put in place partnerships with local public actors:

- **organise** relationships with administrative police authorities (prefects and mayors) in order to assess the threat as well as vigilance and protection measures to be adopted as part of the gathering;
- **co-ordinate** with police forces, *gendarmerie*, municipal police, and firefighters.

If the requirements for public security cannot be satisfied or if circumstances demand it, the organiser can cancel the event.

14- See also sheet 2, page 55.

b) Organise security for the event

The periphery:

- ⊙ prohibit the parking of any vehicle in the area immediately around the site of the gathering;
- ⊙ put signage in place to guide pedestrians at the site of the event and to divert the flow of vehicles;
- ⊙ identify urban furniture that could be used to conceal explosives, remove that furniture, reduce its use, or put in place verification rounds;
- ⊙ call upon law-enforcement agencies or the municipal police to carry out patrols, or even to set up checkpoints and filtering points;
- ⊙ identify high-rise points of vulnerability (overhanging buildings) and make them secure, possibly by using human presence;
- ⊙ if possible, put in place a video-protection system that covers the site's access points as a priority.

The perimeter:

- ⊙ install a physical boundary for the event using interconnecting barriers;
- ⊙ install barriers to organise a route to the checkpoint;
- ⊙ separate entry and exit flows;
- ⊙ at access points, set up checkpoints operated by security officers in sufficient numbers to make entry as easy as possible for members of the public (the quality of filtering can be increased by using magnetometers or walk-through metal-detection equipment);
- ⊙ raise awareness amongst private security officers (vigilance instructions, etc.), and use daily briefings to give reminders of reactions to be adopted in the case of a suspect event, an ill-intentioned act, or terrorist attack. Everyone must know the procedures for raising the alarm and understand them;
- ⊙ provide security agents with radio equipment;
- ⊙ at public access points (entry and exit), set up arrangements (concrete blocks, etc.) aimed at stopping any intrusion by a ram-vehicle;
- ⊙ use human presence to control exit points so that they cannot be used for intrusion;
- ⊙ set up a sufficient number of emergency exits based on the significance of the event, so that the public can be evacuated swiftly in the event of danger within the area.



Inner areas:

- appoint a head of security who will be the sole contact person for police forces, the *gendarmerie*, and emergency services in the event of an intervention on the site;
- call upon the skills of private security companies to ensure the security of such an event;
- when the area is closed to the public, secure it by setting up a human watchkeeping service;
- plan for a central security post to be set up at the heart of the site. That post must be manned 24 hours a day by at least one operator, who will view images from the video-protection system put in place;
- amongst collaborators and exhibitors, raise awareness of threat levels, terrorist operating methods, and detecting identification action. That awareness-raising must be supplemented by information on the behaviour to be adopted in the event of attack;
- install screens and loudspeakers that can broadcast an alert (pre-recorded if possible);
- organise and check deliveries.

1.2.3. Carry out gradual exercises

Exercises involving reaction to an armed attack must be gradual, and they must always give rise to collective feedback that enables lessons to be drawn and procedures to be improved.

Types of exercises:

1. **a straightforward reminder of procedures** and of each individual's role, given by the head of the site or its head of security;
2. **a tabletop exercise** in a room and during which employees present the reaction that they would have in the event of an attack. The session must be given a setting (place, number of assailants identified, and their weapons);
3. **technical test of the alert system**;
4. **organising exploratory reconnaissance missions** (evacuation sites, containment rooms, etc.);
5. **drills with persons simulating intrusion**. Employees must be told that the drill will be held, but they must not necessarily be given its exact date. To avoid any panic, a way must be found to make everyone understand that it is a drill. **Police forces and the *gendarmerie* must be informed that such a drill is being carried out**, and they can be invited to it to contribute their expertise. For such an exercise to be successful, the objectives to be attained must be clearly determined in advance, and a rigorous assessment method must be drawn up. The latter is essential for appropriate lessons to be drawn, and it must be based on a team of assessors who observe the progress of the entire exercise.

2. PREVENTION

2.1. Preventing and flagging up cases of radicalisation

Radicalisation is characterised by “a change in behaviour that may lead some people to extremism or terrorism”¹⁵.

a) Why should I flag up a case of radicalisation?

Radicalisation **concerns all types of ideologies** that may lead individuals to choose violent action in the name of convictions to which they adhere without any possible compromise. That violent action can cause the deaths of other members of the society of which the values and way of life they reject unconditionally.

Thus, we speak of a gradual **process of radicalisation**, with adherence to an ideology and breaking away from one’s usual environment. Radicalisation appears as a phenomenon that is deeply linked to exploitation of conflicts of identity, or frustrations, and of weaknesses. In particular, some terrorist groups seek to enrol individuals who have lost their bearings and who are vulnerable.

The strength of an ideology and its power of attraction must not be under-estimated. Individuals who have developed hatred of our society can adhere fully to a discourse that gives meaning to their frustrations or feeling of humiliation.

Radicalisation is a complex phenomenon that is amplified by the development of social networks. The propaganda carried by individuals or groups touches a range of profiles: delinquents, vulnerable people seeking an identity, people with psychiatric problems, etc. Thus, radicalisation, which is difficult to identify and treat, is a major challenge for national security.

a) How can I identify radicalisation?

Taken in isolation, one of the behaviours listed below does not indicate that radicalisation has occurred. It is the combination of several behaviours that gives a sort of consistency, and that ought to cause surprise.

Some combinations of behaviour or of character traits are strong signals of radicalisation, and they ought to draw your attention¹⁶, whether in your daily environment or in your place of work.

CONSISTENCY → SURPRISE → FLAGGING UP

The signs of breakdown:

- ⊙ physical changes and changes in clothing;
- ⊙ asocial statements;
- ⊙ sudden move to hyper-ritualised religious observance;
- ⊙ rejection of authority and of life in the community;
- ⊙ brutal rejection of daily habits;
- ⊙ turning in on oneself;
- ⊙ self-hate, rejecting oneself, displacing self-hate onto another person;
- ⊙ rejecting society and its institutions (school, etc.);
- ⊙ distancing oneself from family and loved ones;
- ⊙ sudden modification of centres of interest.

15- Information leaflet against radicalisation, a Ministry of the Interior document (MI/SG/DICOM - 04/2015), URL: <http://www.interieur.gouv.fr/Dispositif-de-lutte-contre-les-filieres-djihadistes/Assistance-aux-familles-et-prevention-de-la-radicalisation-violente>, consulted 12/07/2016.

16- Interministerial guide for the prevention of radicalisation, document of the Interministerial Committee for the Prevention of Crime, March 2016, page 103.

The individual's personal environment:

- a weak or even deteriorated paternal or parental image and a weakened environment;
- relationships networks that are already based on dependence on a person, a group, or web sites;
- immersion in a radicalised family.

Theories and discourse:

- conspiracy theories such as references to the end of the world, conspiracy references, and victim-status references;
- veneration of terrorists;
- using hate speech and very violent speech towards a community or a religion;
- proselytising;
- taking part in sectarian religious groups or radical thought circles;
- taking part in conferences given by extremist religious preachers;
- binary behaviour that distinguishes "pure" from "impure".

Techniques:

- using virtual or human networks;
- strategies involving concealment or duplicity;
- planning journeys to war zones.

b) Why launch a flagging-up initiative?

It is a matter of **preventing or even avoiding a tip-over into violent behaviour**, as well as supporting young people and families using adapted cells within the prefectures of the département in which they live.

The aim of flagging up is to **protect the persons concerned by preventing them from committing a criminal act** (to remove those persons as early as possible from the path they have chosen, perhaps in spite of themselves), and to **protect the population** from possible violent behaviour¹⁷.

Taking the initiative by calling the Freephone number is a straightforward act of flagging up. It will be for specialists to assess the seriousness of the case.

c) What happens after a situation has been flagged up?

If the situation is deemed to be of concern by the services of the State, the person who is the subject of the flagging-up and her / his family **will receive specialist support tailored to their situation**.

Your identity will not be revealed; flagging up is strictly confidential. Even if you are not sure of having recognised combinations of signs of suspect behaviour, **you may save lives**. Hence, it is preferable to quickly call the Freephone number. Specialists will take charge of qualifying the situation as being of concern or not.

Flagging up a situation will never be held against you. It is never too late to flag up radicalisation.

Call the freephone number:
0 800 005 696

Complete the online form:
<http://www.stop-djihadisme.gouv.fr/une-question-un-doute.html>

2. PREVENTION

¹⁷- Interministerial Guide for the Prevention of Radicalisation, *op. cit.*, page 7

2.2. Preventing the move to take violent action, and flagging up suspicious situations

Every citizen has a role to play in preventing the move to take violent action. By flagging up dangerous behaviour, you can avoid a criminal act being committed or limit its scope, and thus save lives. All citizens have the right to be protected, but they all have the duty to act.

2.2.1. Why flag up a suspect situation?

In a particularly heightened context of terrorist threat, it is more than ever necessary to be attentive on a daily basis to the world around us.

Organising an attack most often requires preparation work as well as human and material means. **Most terrorist attacks first involve terrorists getting their bearings** to identify the security measures that have been put in place so that they can be bypassed, access routes, etc. In the course of the various phases of setting up such an operation, **the terrorists are forced, at one time or another, to reveal themselves.**

By being attentive to their daily environment, all citizens can note and flag up facts, objects, or behaviours that could indicate a possible move to action. Experience has shown that simple signs identified by a passer-by or a neighbour could help prevent a terrorist act.

Attention paid
by each person
to simple details
saves lives.

2.2.2. How can a suspicious situation be detected?

Certain behaviour or situations may seem inconsistent in a given environment. You must question those inconsistencies and wonder if they are worthy of being flagged up.

Preparing for a terrorist act is not always as perfect as one may imagine, or as one may see on television. Inconsistencies appear, and you can detect them. **Call upon your common sense and your intuition.**

Thus, detecting suspect behaviour is a matter of knowing how to question the inconsistency between a detail and a situation, or the mismatch between a person's attitude and a place. **Any inconsistency that makes you think that a violent act is being prepared must make you take note, it must make you question, and it must lead you to flag it up.**

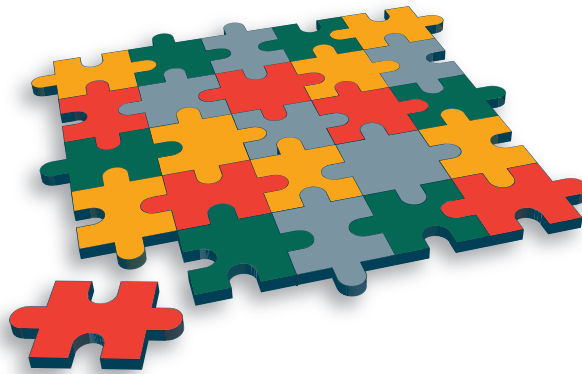
Hence, you must learn to observe your environment (neighbourhood, professional life, public transport, etc.).

INCONSISTENCY → QUESTIONING → FLAGGING UP

How is a terrorist act planned?

Understanding how a violent act is planned can help you to identify some signs of preparation. Regardless of terrorists' level of experience, they will prepare for their act as follows: choice of targets, preparing for the act, and setting up.

Preparation work for a terrorist act leaves a set of clues that, like the pieces of a puzzle, can be assembled by the security forces to frustrate a planned attack.



a) The choice of targets

Terrorist acts can be aimed at symbolic targets (personalities, a community, a trade representing the State, etc.) or they can be indiscriminate (the population as a whole), to create a climate of fear and affect the economic interests of the country.

b) Preparing for the act

Terrorists necessarily carry out reconnaissance work relating to the intended target, in order to identify vulnerabilities and to determine the method of action that will enable them to attain the intended objective:

- **physical reconnaissance of the site targeted**, alone, in tandem, or in a group (possible communication by gestures, timing, a single person present at the same place several times for no apparent reason, a vehicle parked for long periods with people in it, etc.);
- **gathering a maximum amount of information** on the target:
 - seeking internal collusion;
 - requests for information concerning security measures through apparently innocent conversations;
 - observing how security checks are carried out, or even testing those checks by using false alarms (of the bomb-alert type);
 - taking pictures (photography or film) of the infrastructures of the site targeted and of the security arrangement put in place (a ministry's entrance door, soldiers on patrol, etc.);
 - making notes on security arrangements (site plan, positions of surveillance cameras, entry and exit doors, etc.);
 - searching for information on the internet (social networks, aerial layouts and views, etc.);
- using **concealment or camouflage techniques** (that can be identified by the immediate circle): using pseudonyms or multiple forms of identification with different names, using pre-paid telephone cards or several mobile telephones, etc.

c) The phase before action

An individual who is on the point of committing a terrorist act may conceal weapons: a knife, an assault rifle, a handgun, an explosive belt, ammunition, etc. Hence, that person will wear adapted clothing, and may:

- carry a bag that is abnormally heavy, or that is mis-shaped by a weapon;
- wear protection (knee pads, a bullet-proof jacket);
- wear clothing that is wrong for the season, or sufficiently bulky to conceal a weapon;
- conceal a weapon behind the back to cross a checkpoint that involves opening jackets with no pat-down;
- show signs of nervousness or wariness in contrast with the environment.

An attack involving explosives can also be carried out. Certain situations should alert you:

- a letter or parcel with a badly-written address, that bears marks, or that gives off odours may contain explosives;
- an abandoned parcel or bag. A bag left in a main passageway must be flagged up;
- a vehicle that has been left parked for a long time near a place where people gather (a market, a place of worship, etc.) or a sensitive site (town hall, embassy, etc.). A booby-trapped vehicle will never be put in place at random; it will be near the target aimed at. A vehicle without number plates should make you take notice.

2.2.3. How can I flag up and react?

a) For all citizens

If you witness suspicious behaviour, remain discreet. Do not show the person identified that her / his attitude surprises you. **Observe and memorise objective elements** that can be passed on to the police or to the national *gendarmerie* (registration plates, vehicle model, precise description of individuals, direction of flight, etc.). So that your description can also be useful to internal-security forces, the objective elements that you give are absolutely essential.

OBSERVE → MEMORISE → FLAG UP

Call the internal-security forces by dialling 17, 112, or 114 (for people with hearing or speech difficulties).

In the event of an emergency aboard a train:

- **call 31 17 or send a text message to 31 177.** If you call using the **Alerte 3117 app**, the person who deals with your call will geolocate you. Describe the place of the attack: the train number or its geographical position, the wagon number, etc.

b) For employees of a sensitive site or a site that deals with the public

Internal procedures must allow a description to be passed up the chain swiftly.

If an employee observes suspicious actions or behaviour, she / he:

- can strike up an informal conversation with the individual whose behaviour has been noted;
- must inform her / his superiors.

By asking open questions¹⁸, the employee will be able to determine if the individual identified by her / his behaviour is concealing ill intentions. In the event that an individual is preparing to carry out an ill-intentioned act, that individual may behave in an elusive, nervous, or aggressive manner.

For example, if an unknown individual is found inside an area that is not open to the public, the employee may ask whom that person wishes to meet. Similarly, if an individual takes photos that give the impression of reconnaissance being carried out, the employee can ask what has aroused the individual's interest.

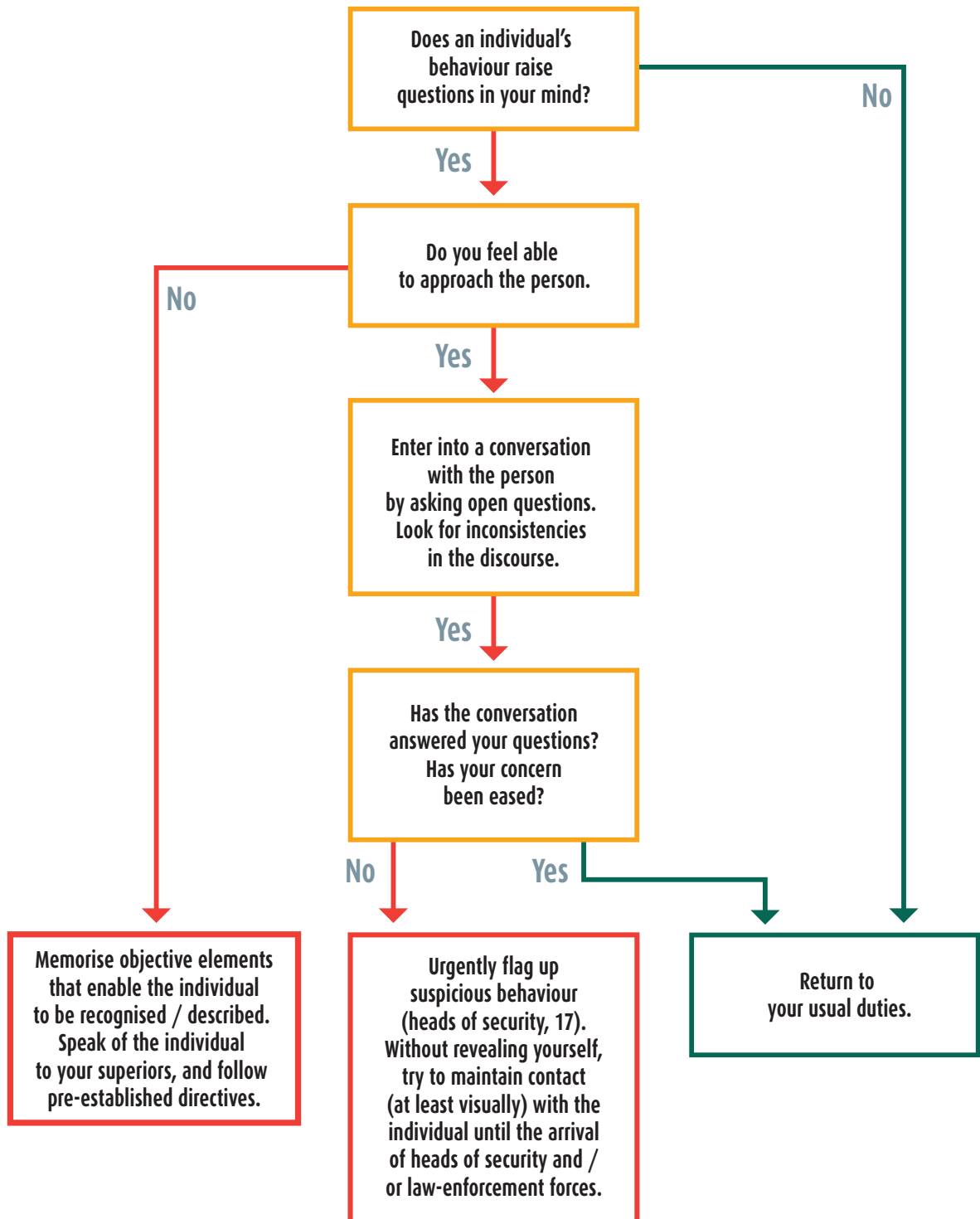
Employees, especially those in charge of the security of assets and of people, must be made aware, to the extent possible, of those types of situations and of the reactions to adopt.

Operators must raise awareness amongst their employees by specific drills that enable them to acquire good reactions and attitudes.



18- Questions that you cannot answer by saying "yes" or "no".

Example of a decision-making support for an employee of a sensitive site or a site that deals with the public, and who is faced with suspect behaviour.



2.2.4. What can be done about drone overflights?

Drones are considered toys, but they are a threat that must be taken very seriously. Ill-intentioned persons can use them to collect information with a view to preparing to commit a terrorist act. Moreover, we must not forget that a drone can also be used as a weapon because of its carrying capacity (grenade, chemical or biological weapon, etc.), or even an improvised weapon.

a) What is an ill-intentioned drone?

Civilian aircraft operating without anyone on board, commonly called drones, are governed by two decrees passed on 17 December 2015¹⁹. By virtue of the latter, and except any derogations, it is especially prohibited to cause a drone to overfly public areas in built-up areas, and to cause a drone to overfly anywhere at night.

Thus, a drone overflying a gathering of people of operating at night must be considered potentially ill-intentioned. Only potentially, because it may be case of an unintentional act of negligence or clumsiness on the part of a "leisure" remote pilot²⁰.

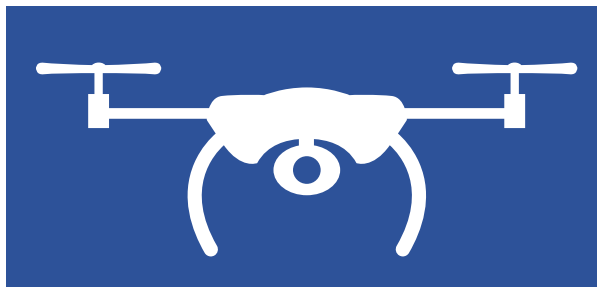
b) Who should be warned?

In the event of an abnormal situation, alert the security forces (17).

However, take care not to burden the authorities. Information must be relevant, especially in the case of night overflights.

c) What must be described? (non-exhaustive list)

- ◉ Where? When? What? How many?
- ◉ The flight altitude, its departure point, and its direction.
- ◉ The type of drone (multirotor or flying-wing, electric propulsion or thermal propulsion, type of lights).
- ◉ Is it carrying an external load (camera or other)?
- ◉ If the remote pilot has been found, provide a physical and behavioural description.



19- On those 2 decrees, see "For further information" section, page 70.

20- The remote pilot is often within sight of her / his drone, i.e. within a radius of less than 500 m of the device. Depending on her / his behaviour, it may be possible to determine the nature of the overflight.

3. REACTION

3.1. What can be done in the event of an armed attack?

An armed attack is one that is carried out by one or more individuals whose intention is either to cause a maximum number of victims indiscriminately or to specifically target certain persons or symbolic places.

The attackers can mainly use firearms, cold weapons (knife, axe), or explosive belts.

The recommendations that you will read below will be easier to apply if drills have been carried out beforehand.

3.1.1. General case

Determine the most appropriate response to the situation. That situation is not a fixed one, it changes, so adapt your methods of reaction to circumstances.

If the attack is external to the site where you are, it is recommended that you remain sheltered.

If the attack takes place within the site where you are, comply with the security instructions given below.

a) Escape

Condition 1: Be certain that you have identified the exact location of the danger.

Condition 2: Be certain that you can escape without risk.

In all cases:

- ◉ do not set off the fire alarm;
- ◉ leave all your belongings behind;
- ◉ do not reveal yourself (bend over, lean forwards);
- ◉ take the least exposed and closest exit;
- ◉ use a known route;
- ◉ if possible, help others to escape;
- ◉ warn / alert other people around you;
- ◉ dissuade anyone from entering the danger area



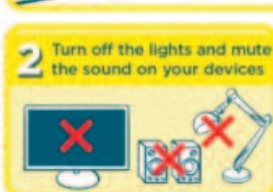
REACTING IN THE EVENT OF A TERRORIST ATTACK

THE FOLLOWING ACTIONS COULD SAVE YOU BEFORE THE ARRIVAL OF THE SECURITY FORCES

1/ ESCAPE

If this is not possible

2/ HIDE



3/ ALERT

AND OBEY THE ORDERS OF THE SECURITY FORCES

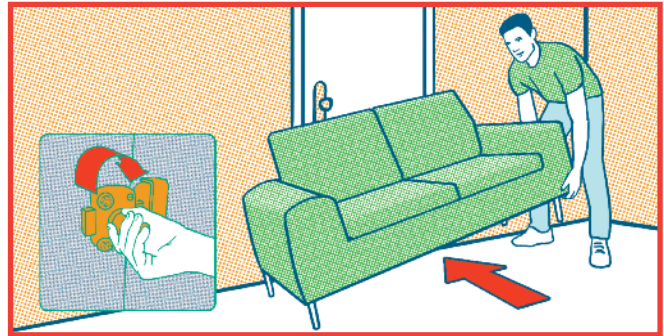


VIGILANCE

- If you witness a situation or **any behaviour you consider suspicious**, you should contact the security forces (17 or 112)
 - When you enter a venue, **locate the emergency exits**
 - Do not publish any information on the security forces' operations
- Do not circulate rumours or any **unverified information** on the Internet and social networks
- Follow the **@Place_Beauvau** and **@gouvernementfr** accounts on social networks

b) Lock yourself in

- ◉ If you cannot escape, **lock yourself in, barricade the entrance**, hide yourself in a place that is beyond the reach of the attackers;
- ◉ **block the door**, if it has no lock, by blocking the handle with whatever you can (furniture, etc.);
- ◉ **switch off the lights;**
- ◉ move away from walls, doors, and windows;
- ◉ **lie down on the ground** behind several solid obstacles (projectiles shot through partitions can reach the inside of the room where you are);
- ◉ **maintain complete silence** (mobile telephones in silent mode with no vibrator) and disconnect landlines telephones;
- ◉ remain close to people showing signs of stress and reassure them;
- ◉ await intervention by the security forces.



c) Alert

Once you are safe:

- ◉ warn the security forces [17, 112, or 114 (for people with hearing or speech difficulties)], and try to provide essential information:
 - **Where?** Give your position and that of your attackers;
 - **What?** The nature of the attack (explosion, shooting, hostage-taking, etc.), type of weapon (firearm, cold weapon, explosives, etc.), estimated number of victims;
 - **Who?** Estimated number of assailants, description (sex, clothing, facial features, distinguishing marks, etc.), attitude (how are they behaving, are they watching television, do they have means of communication, etc.). Estimated number of wounded persons and of persons hiding around you.
- ◉ If you cannot speak, call and leave the line open so that the security forces can be warned.



DON'T THINK THAT OTHERS HAVE GIVEN THE ALERT – DO IT YOURSELF!

d) Resist

If remaining hidden or carrying out an evacuation are impossible, and if your life is directly threatened, then to the extent possible, **resist as a last resort**.

Collective action to take the upper hand over an isolated adversary can turn the situation around.

Simple actions can help to interrupt or neutralise the threat, as follows:

- ◉ distract the adversary (shout out) and attack;
- ◉ take advantage of a moment of vulnerability affecting the attacker (changing a charger, etc.);
- ◉ throw objects / use improvised weapons.

Be careful. Hostage-taking is different from a mass shooting. Do not seek to confront terrorist, and comply with their instructions.

e) Facilitate intervention by the security forces and the emergency services

In order to facilitate intervention by the security forces and the emergency services:

- ◉ stay locked in until the security services carry out the evacuation;
- ◉ **evacuate calmly, with your hands open** and in full view so that you are not seen as a suspect;
- ◉ **do not run towards the security forces;**
- ◉ **point out the wounded** and their location, and if you have received first-aid training, provide first aid;
- ◉ do not leave the location straight away, as your evidence may help the enquiry.



3.1.2. Special cases

a) In the event of an attack with a cold weapon

- ◉ **run away;**
- ◉ **if you cannot run away**, protect yourself using an improvised shield (bag, chair, an item of clothing rolled around a forearm, etc.);
- ◉ **use an improved weapon** that enables you to extend your reach;
- ◉ **attack as a group:** one person can attract the attacker's attention whilst another tries to neutralise her / him.

An attacker with a cold weapon can be put off balance by a group reaction from victims or nearby people. To the extent possible, get together to plan before attack, and launch a surprise attack.

b) In the event of an explosion or of an explosive risk

- ◉ move away from the site of the explosion;
- ◉ do not touch anything (object, abandoned bag, debris);
- ◉ protect yourself / take shelter behind a solid obstacle (a second explosion close to the site of the first and aimed at the emergency services or the security forces is possible);
- ◉ await intervention by the emergency services.

c) In the event of an attack on a train**Hide**

Lie down under the seats, or crouch down.

Alert

Call 31 17 or send a text message to 31 177. If you call using the Alerte 3117 app, the person who deals with your call will geolocate you. Describe the place of the attack: the train number or its geographical position, the wagon number, etc.

Resist

As a last resort, if your life is in danger, impede or neutralise the terrorists' actions with the help of people hiding around you.

Escape

Do not leave the train unless you can do so without crossing a railway line.

Facilitate intervention by the security forces and the emergency services

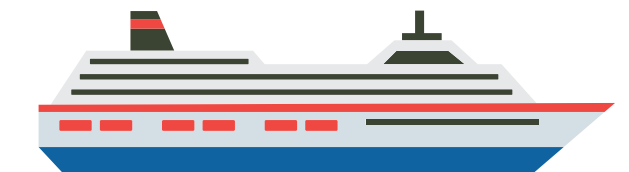
When the law-enforcement agencies arrive, put your hands in the air and stand still.

d) In the event of an attack on an underground railway**Call 31 17 or send a text message to 31 177.**

Use the calling points on station platforms to make contact with officials.

e) In the event of an attack on a vessel at sea**Get away from the threat**

- if the size and architecture of the vessel allow it, get away from the place of the attack and leave your belongings behind;
- do not jump into the water.

**Follow onboard instructions.****Hiding**

- if you are far from your cabin, hide, lock yourself in, and avoid crowds;
- if you are near your cabin, lock yourself in your cabin;
- if you have managed to lock yourself into a room, block the entry, close the doors, hide, and do not open the doors for any reason;
- conceal your presence: turn off all sources of light and sound.

ATTENTION: Do not switch off your telephone. Put it into silent mode

3.2. What can be done in the event of a cyberattack?

During an attack

In the event of a cyberattack, **report the facts quickly** to the specialist services via the **PHAROS²¹** platform, or by telephone to the dedicated number.



After an attack

If you have been the victim of a cyberattack, in addition to making a report, **lodge a complaint** at a department of the national police or the national *gendarmerie*, or send a letter to the State Prosecutor at the competent High Court.

Provide yourself with a maximum amount of information on the attack observed. Thereafter, specialist departments will take over the investigation. Do not hesitate to check the "risques.gouv.fr" web site for information on the various behaviours to adopt based on the type of attack of which you may have been a victim.

Finally, be attentive to instructions and recommendations given by the authorities concerning best practices to be adopted on the internet.

Cybervigilance

In a crisis, information circulation is an essential part of good management of events. Being cybervigilant also means taking care not to circulate wrong information that may change the management of the crisis. **During an attack, do not pass on rumours under any circumstances.**

- Be attentive to instructions from official sources:
 - the *Agence nationale de la sécurité des systèmes d'information* (ANSSI – National Agency for the Security of Information Systems): technical recommendations following a cyberevent;
 - the government information service, the Ministry of the Interior (*gendarmerie*, police, prefecture), and local authorities;
 - other ministries affected by the crisis.

21- Reporting site: <https://www.internet-signalement.gouv.fr/>

3.3. What can be done in the event of an attack using a toxic product?

Several toxic products are used in industry (chlorine, for example). Some of them have already been diverted by terrorist groups for warfare purposes. These products are likely to be intentionally released in high-traffic areas.

Toxic products can penetrate the organism in different ways. **Through inhalation, contact with the skin or the eyes, or by swallowing, they can cause serious injuries:** burns, pulmonary oedema, asthma, etc. Those injuries can be limited or even prevented by adopting the useful steps detailed in the infographic on the following page:

- **remain calm, and move to a safer place as soon as possible** whilst helping more vulnerable people (images from 1 to 4);
- **limit poisoning by getting undressed** and by washing yourself, in order to reduce or eliminate the toxic product so that it no longer constitutes a risk. Prevent it from spreading to other people (image 5);
- **contact the emergency and medical services as soon as possible by calling 15, 18, 112, or 114** (image 6);
- **stay where you are so that you do not contaminate other people**, including emergency and medical staff, wait for the emergency services so that they can give you first aid (images 7 and 8);
- **in all cases, do not drink anything, do not rub your face, do not eat, do not smoke, and avoid contact with other people** (image 9).

WHAT TO DO IF YOU ARE EXPOSED TO TOXIC FUMES

WHILE WAITING FOR THE EMERGENCY SERVICES TO ARRIVE, THESE FEW STEPS COULD SAVE YOUR LIFE

1 Protect your nose and mouth by any means possible: damp handkerchief, scarf or fabric.

2 Even if you're feeling unwell, don't lie or sit down - you might not be able to get back up again.

3 Quickly leave the area that seems to be worst affected (an odd smell, if people's eyes are watering or they suddenly start feeling unwell for example).

4 If you notice people fainting or having difficulty breathing, help them to leave the area without turning back.

5 Once a safe distance away, carefully remove your first layer of clothing without touching the outside surface and try to put it somewhere out of the way - preferably in a plastic bag (like a bin liner) or, failing that, on the ground away from you and point it out to the emergency services when they arrive. If you are able to, strip off completely and wash your hands with soap and water.

6 Only use your mobile phone to call the emergency services by telling them your location and if there is a need for swift assistance in a serious situation.

Brigade fire: 18
European emergency number : 112
Emergency Medical Assistance Service (SAMU): 15

18
112
15

114

7 Whatever you do, don't go home. Don't head to the hospital of your own accord. Make sure you wait for the emergency services and follow their instructions, otherwise you risk contaminating those around you too!

8 The emergency services will organise an assembly point where you will receive the necessary care.

9 Avoid physical contact with other people, don't drink, try not to rub your face, don't eat and don't smoke.

STAY CALM, THIS WILL MAKE THE EMERGENCY RESCUE AND MEDICAL TEAMS' WORK EASIER

IMPORTANT !

Some serious symptoms may only appear several hours after exposure.

In this case, dial 15 as soon as possible, explain that you were in the contaminated area and follow the instructions you are given.

On social networks, follow the accounts @Place_Beauvau and @gouvernementFR. Listen out for instructions from the public authorities.



For more information: www.gouvernement.fr/ia

4. MANAGING THE POST-ATTACK SITUATION

4.1. If you have witnessed a terrorist attack

Contact the police and the *gendarmerie* to report what you saw at the site of the attack, and give all the details that may help with the investigation. Any photos or video footage that you manage to take during an attack should only be passed on to the authorities.

4.2. If you have been the victim of a terrorist attack

Following a terrorist attack, victims are dealt with by the emergency services. Thereafter, they benefit from a strengthened arrangement for providing help to victims, and they receive compensation. That arrangement is steered by the Secretariat of State tasked with helping victims.

4.2.1. Being dealt with in an emergency

At the site of the terrorist attack or nearby, you can make yourself known to the police and the *gendarmerie* or to the emergency services. Medical / psychological assistance cells are tasked with dealing with you and to carry out an initial intervention, the main aim of which is to reduce the risks of post-traumatic shock.

In the event of a large-scale terrorist attack, the Prime Minister can activate the Cellule interministérielle d'aide aux victimes (CIAV – Interministerial Cell for Supporting Victims). It is tasked with informing victims and their families of the arrangements that have been put in place and of their rights. A reception centre for families and various centres for offering medical / psychological help may be set up.

4.2.2. Help for victims of terrorism

To respond to victims' expectations and needs, a Secretariat of State tasked with helping victims, placed under the authority of the Prime Minister, was set up in France in March 2016. It is tasked with protecting and ensuring victims' rights. In the event of a terrorist attack, victims are offered specific and protective arrangements.

To obtain information, receive an explanation of what to do based on the situation (losing someone close, physically- / psychologically-wounded, someone close to a wounded person, etc.), to receive guidance (receive psychological help, lodging a complaint, making funeral arrangements, compensation for damage, organising the inheritance, etc.), and compile a file, you can:

check the web site set up to simplify formalities for victims of terrorist acts:

<http://www.gouvernement.fr/guide-victimes>

The site allows victims to:

- get to know the formalities and to carry them out on line;
- make and monitor a request to the Fonds de garantie des victimes des actes de terrorisme et d'autres infractions (FGTI – Guarantee Fund for Victims of Acts of Terrorism and other Offences) and to the *Office national des anciens combattants et des victimes de guerre* (ONAC-VG – National Agency for Armed-Forces Veterans and for Victims of War);
- find contact details for victim-assistance associations.

Call 08 842 846 37 (7 days a week)

The platform is a single entry point for all victims, and will guide you to one of the 132 victim-assistance associations accredited by the Ministry of Justice across the whole territory. The professionals of those associations, jurists, psychologists, and social workers, are tasked with attending to you free of charge to:

- listen to you and provide you with information on all the entitlements that you enjoy, on the functioning of the law, and on the compensation arrangements for victims of terrorist acts;
- facilitate the formalities that you have to carry out with bodies such as the FGTI, the ONAC-VG, the CPAM (*Caisse primaire d'assurance maladie* – Primary Health Insurance Fund), the CAF (*Caisse d'allocations familiales* – Family Benefits Fund), and the tax administration;
- offer you psychological support following on from the emergency help that you may have already been given;
- guide you towards professionals (lawyers, medical consultants, etc.).

Contact SAMU (15)

Victims of a terrorist attack can receive medical / psychological support everywhere in France. By calling 15 (24 hours a day), SAMU (*Service d'Aide Médicale Urgente* – Emergency Medical Assistance Service) will redirect your call to a cellule d'urgence médico-psychologique (CUMP – Medical / Psychological Emergency Cell). The CUMP will be able to deal with you, and, if needed, it will be able to offer you long-term monitoring in your département's public structures.

4.2.3. Compensation for victims of a terrorist act: the FGTI

Under certain conditions, victims of a terrorist act can receive compensation from the *Fonds de garantie des victimes des actes de terrorisme et d'autres infractions* (FGTI).

For further information, go to:

<http://www.fondsdegarantie.fr/actes-de-terrorisme>

4.2.4 Lodging a complaint

In France, you can lodge a complaint at the *police judiciaire* (Criminal Investigation Department) office that is closest to your domicile. To find out where that office is, you can telephone the police station or the *gendarmerie* brigade that is closest to your domicile to be given the details of the closest police judiciaire office.





PART 3

AREAS OF ACTION

This part aims at detailing the specificities of each of the VIGIPIRATE plan's areas of action.

1. ALERT AND MOBILISE

Description of the area



Giving the alert aims at **passing information on urgently to all the actors concerned, in order to immediately mobilise means of intervention and adapt protection measures**. It also involves getting the population on side by using messages to maintain constant vigilance and to bring about public mobilisation in the event of a serious event.

Some activity sectors have their own chains. Those alert chains connect the ministries concerned, the State's decentralised administrations and departments, and

operators. Operators of vital importance have specific legal obligations in matters of alerting and intervening.

Security strategy

The security strategy is a response to a dual purpose of information and responsiveness. It aims at **alerting and communicating as widely as possible, whilst mobilising specialist national means (such as the ability to fight the threat of spreading toxic products)**.

By way of example, as part of preparations for Eurofoot 2016, significant specialist means involving civil security, the internal security forces, the SAMU, and the armed forces were placed on alert or deployed.

2. PROTECTING MASS MEETINGS

Description of the area



A gathering involves a public grouping of a significant number of people in an open space. Protecting gatherings involves several types of actors: **the organisers, the administrative authority** (mayors, prefects), **law-enforcement agencies** (police, *gendarmerie*, municipal police).

Organisers are responsible for the general security of the gathering, especially the security of participants. An in-house security service must ensure that the gathering proceeds appropriately (access-filtering, checking people, security guards), and will liaise with law-enforcement agencies. The security service may be drawn from the private sector.

The administrative authority is responsible for public order. It checks the measures planned by the organisers in light of the nature of the gathering, the number of members of the public expected, the site configuration, and the circumstances that are unique to the event. In the event of a risk of breach of the peace or of a particular threat to a gathering, the administrative authority can prohibit the gathering by means of a ruling that it notifies immediately to the organisers.

Law-enforcement agencies can be used subject to a decision by the administrative authority, and based on the nature or vulnerability of a gathering, for work involving traffic management, crowd management, and general surveillance.

Security strategy

The strategy involves setting up **surveillance and control arrangements based on the principle of in-depth defence**. As a last resort and based on the threat, the decision can be taken to restrict or even prohibit the gathering.

To determine the level of protection of a gathering, it is essential to assess the threat to which it is exposed. Thus, particular attention must be given to gatherings that involve large numbers of people, tourist significance, and cultural, religious, or political symbolism. VIGIPIRATE stance memos have the particular aim of identifying the most sensitive categories of gatherings for a given period.

3. PROTECTING INSTALLATIONS AND BUILDINGS

Description of the area

The area that covers installations and buildings involves **all buildings that may be potential targets, whether because of their symbolic, economic, political, or ecological value, or because of the public that they deal with.** Certain infrastructures that are specific to precise areas of activity are given specific protection that is described in the classified chapters of the VIGIPRATE plan that cover them. That is the case for transport, dangerous installations, networks, the food chain, and health.

The public authorities are tasked with providing external protection, which they do through surveillance, traffic management, and parking management. The arrangement is tailored to the type of installation, its configuration, and the threat assessment. It can use various law-enforcement agencies: local services, municipal police forces, the national police, the national *gendarmerie*, or even the armed forces.

The heads of installations and buildings are tasked with internal protection and with access to buildings.



Security strategy

The strategy aims at **adapting external security by acting on surveillance as well as on parking and traffic conditions around installations, the security of access points, and flow control.** It is based on the principles of in-depth defence and of responsibility shared between the operators of installations and public authorities. The VIGIPRATE stance memos specify the categories of buildings that must be covered by particular vigilance or protection.

Finally, to traditional measures for the security of buildings must be added procedures that are known to all and that enable the best possible reaction by all staff in the case of an ill-intentioned intrusion or even a terrorist attack. **The quality of an establishment's preparation work affects the quality of its reaction in a crisis.**

4. 4PROTECTING DANGEROUS INSTALLATIONS AND MATERIALS

Description of the area

The VIGIPIRATE plan covers industrial activities as well as the storage and transport of certain materials, due to the risks they cause because of their dangerous nature.

The public authorities define the regulation that is applicable in this area, check that it is properly applied, and grant operating permits.

In the particular case of the civil nuclear sector, verification is done by the Autorité de sûreté nucléaire (ASN – Nuclear Safety Authority), which is an independent authority.

The VIGIPIRATE plan brings together businesses in the area that have security obligations: those that are classified as SEVESO “Lower Tier” and “Upper Tier”, those with activities that are subject to authorisation, and those that transport dangerous materials. In particular, they are businesses in the chemical, hydrocarbon, and nuclear sectors.

The general public is also covered by regulation on the marketing and use of products that can be used to make explosives.



Security strategy

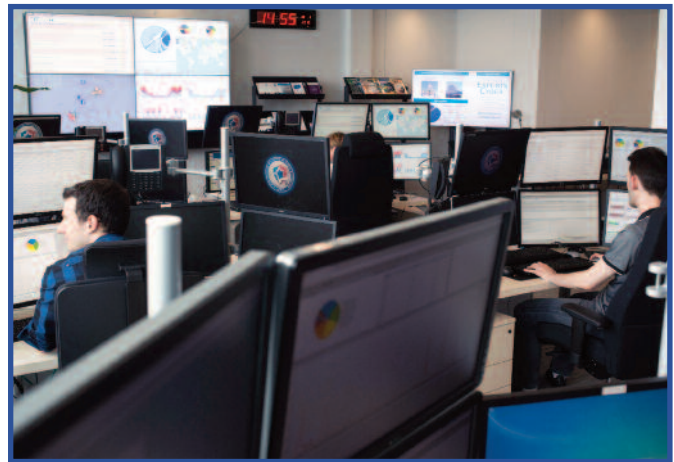
The strategy aims at **protecting dangerous installations**, places where dangerous or sensitive materials are stored, and the transport of those materials.

In addition, protecting those installations involves ensuring that no ill-intentioned act can have major consequences on populations and the environment.

5. ENSURING CYBERSECURITY

Description of the area

In the age of digital technology and dematerialisation, **information systems have become a choice target for terrorists**. Furthermore, attempts to disrupt their proper functioning through information-technology attacks can have heavy consequences nationally by attacking the lives and the health of citizens, by disrupting or disorganising society, by causing significant financial losses, and by upsetting the functioning of our economy.



To protect that vital sector, a cybersecurity arrangement that is specific to the VIGIPIRATE plan has been put in place. It involves several actors:

It involves several actors:

- ◉ The *Agence nationale de la sécurité des systèmes d'information* (ANSSI) organises and co-ordinates the implementation of the cybersecurity part of the VIGIPIRATE plan. It is based on the ministry that co-ordinates each of the sectors of vital importance;
- ◉ *opérateurs d'importance vitale* (OIV)²² apply information-technology security measures that are specific to their sector, and they must also ensure that those measures are applied appropriately by their subcontractors;
- ◉ administrations as a whole, as entities responsible for the State's information systems, implement the instructions of the VIGIPIRATE plan that are incumbent upon them;
- ◉ local authorities and non-OIV operators are encouraged to implement the VIGIPIRATE plan;
- ◉ citizens who, on a daily basis, in their professional or private lives, deal with information systems, are invited to apply the essential rules of precaution and vigilance.

Security strategy

The strategy consists of a **permanent security stance (cybersecurity)**, as well as incorporating **reinforced-protection measures tailored to changes in the threat (cyberdefence)**.

²²- For further details, see the "Glossary", page 73.

6. PROTECTING THE AIR SECTOR

Description of the area

The air sector covers **activities that protect or use national airspace, all associated infrastructures, and all French and foreign aircraft, as well as air-transport users and professionals.**

The State is a major actor in its protection. The Minister of Transport is the competent authority in matters of civil-aviation security. In that regard, the Minister is responsible for co-ordinating with the other administrations concerned, draws up and facilitates State policy, and ensures that it is applied by the various air-transport actors and operators. The Minister represents the government in European and international consultative bodies.



Implementing security measures is the responsibility of private actors (aerodrome operators, air-transport companies, accredited agents), with the surveillance of that implementation being carried out by the Ministry of Transport, the Ministry of the Interior, and the Ministry of the Budget.

Under the direct authority of Prime Minister, the air force defends national airspace and its approaches. That mission consists of enforcing sovereignty and opposing its use by a possible aggressor. That arrangement is supplemented by bilateral agreements with bordering countries.

The VIGIPIRATE plan brings together several actors beyond the scope of the State alone, actors that, to varying degrees, have obligations in matters of safety and security or who can contribute to them. They may be covered by national regulations, by directives, or by specific recommendations as part of protection against the terrorist threat. In particular, they are air-transport businesses, aerodrome operators in Metropolitan and Overseas France, security services, and services with national competence in matters of air navigation and of meteorology.

Security strategy

The strategy aims at **protecting users and professionals of air transport and aeronautical installations, national airspace, and aircraft, as well as ensuring that areas accessible to the public and to airport professionals receive the requisite level of vigilance.**

The objective is to ensure the best possible consistency of protection measures relating to the various components of the air sector, as well as protecting passengers, accompanying persons, and air-sector professionals.

7. PROTECTING THE MARITIME SECTOR

Description of the area



Maritime areas under French sovereignty cover almost 11 million km² across the regions of the world. Maritime transport covers **the activities of vessels and infrastructures, ports, and port-based support installations.**

Protecting the maritime sector brings together various actors. The representatives of the State (maritime prefect in Metropolitan France, prefect or high commissioner of the Republic overseas) ensure the maintenance of France's sovereignty over its maritime areas, and they

co-ordinate the work done by the various administrations that intervene at sea. The commander of a sea area is responsible for implementing the maritime defence of the territory. In that regard, she / he ensures the surveillance of the approaches.

The VIGIPIRATE plan brings together actors beyond the scope of the State alone, actors that, to varying degrees, have obligations in matters of safety and security or who can contribute to them: public and private port operators whose infrastructures provide management of the land / vessel interface, persons responsible for management of their vessels, and all activities dedicated to vessels and ports.

The maritime transport of goods represents 90% of worldwide exchanges, so it plays a strategic role in France's economic activity. Its main vulnerabilities are linked directly to the commercial nature and international dimension of its activities, as well as the nature of its infrastructures: the high level of passenger and goods flows, deadline requirements, the number of containers and their general use, ease of access to port installations, insertion of ports into towns and cities, and freedom of movement around vessels.

Security strategy

The strategy aims at **protecting the maritime area of territorial waters, vessels, reserved areas, and the sensitive components of ports and port installations, as well as ensuring that the public areas of those ports receive the requisite level of vigilance.**

8. PROTECTING LAND TRANSPORT

Description of the area



The area of land transport includes **all means and bodies involved in public and rail transport, as well as linear transport infrastructures.**

The infrastructures include not only physical infrastructures (roads and railways) but also information systems used to operate them (signalling, traffic management, information for users, and pricing) and nodal interchanges.

The Minister of Transport oversees the various actors of the area that all play a role in protecting it to the

extent of their responsibilities, and that are essentially infrastructure administrators and businesses with an activity that is national in scope.

Security strategy

The strategy aims at **protecting passengers in stations, trains, and urban public transport. It also aims at protecting the sensitive components of land transport** as well as certain stations.



9. PROTECTING THE HEALTH SECTOR

Description of the area

The health sector brings together **all actors and activities that provide healthcare, health supervision and security, as well as the production and distribution of healthcare products, enabling prevention, and, where necessary, to deal on a massive scale (including from a medical / psychological perspective) with people following a terrorist act (including NRBC-E²³).**

Protecting the sector involves various actors. The Ministry of Health coordinates the functioning

of the sector through its directorates general (Directorate General of Health, Directorate General of Healthcare Provision, etc.) and through the work of health agencies (regional health agencies and regional agencies offering health expertise). Biomedical and toxicology laboratories also play a role in the supervision arrangement. Pharmaceutical businesses and wholesale distributors are involved in securing the supply of healthcare products. Finally, self-employed healthcare professionals are the first link in the healthcare chain, which includes a wide variety of public and private medical / social establishments.



Security strategy

The strategy aims at:

- **encouraging the general use of internal security plans in healthcare establishments, and “health – security – justice” agreements²³, which are a permanent stance of vigilance and security in the healthcare sector;**
- **adapting the health-supervision and health-security arrangement to the risks that our country has to deal with;**
- **securing the capacity to produce and distribute healthcare products, as well as water intended for human consumption.**

²³- See “Glossary”, page 72

10. PROTECTING THE FOOD CHAIN

Description of the area



The food chain is defined as **all businesses involved in production and transformation, as well as centres for bringing to market products intended for human or animal nutrition.**

The agrifood sector is now highly internationalised, and is experiencing growing complexity in production systems, constant changes in supply modes, and constant technological developments. It is characterised by a wide diversity of sectors that include a large number of small businesses beside large businesses, including many multinationals.

The essential sectors include:

- agrifood industries, which account for over 13,000 businesses except for commercial craft products, with a significant place being reserved for transforming livestock products;
- large-scale food distribution, involving 10 large national groups and over 12,000 establishments in Metropolitan France.

Security strategy

The strategy aims at **encouraging the general use of plans de sécurité interne (PSI – Internal Security Plans)²⁴. Those plans cover six areas: the physical protection of access points, the control of traffic flows (people, vehicles, and products), the safety of the staff of the establishment, and stock management, as well as information-technology processes and security.**

In businesses of the sector, those plans form a permanent stance of vigilance and security. In addition, they can be adapted based on alerts and / or a more precise characterisation of the threat.

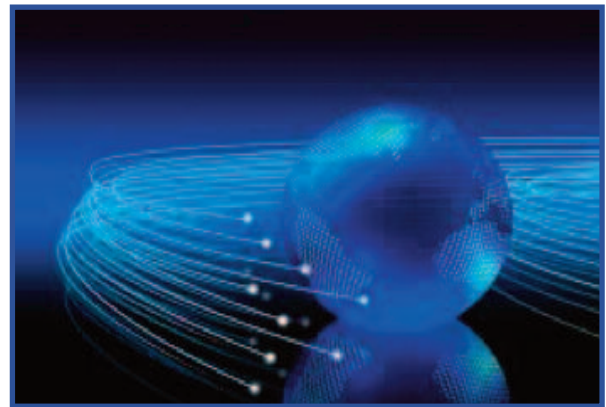
²⁴- For further details, see the “Guides to best practice” section, page 71.

11. PROTECTING NETWORKS

11.1. Protecting electronic-communication and audiovisual networks

Description of the area

The area of electronic-communication and audiovisual networks includes **all activities, operators, and installations that route electronic communications**, i.e. the broadcasting, transmitting, and receiving of signs, signals, written material, images, and sound electromagnetically (fibre optic, cable, terrestrial, or satellite). It includes fixed-line and mobile telephony, fixed and mobile data services, including access to the internet and to so-called "social" networks, and the broadcasting of television and radio programmes.



Two actors contribute to protecting the area:

- **the *Commissariat aux communications électroniques de défense*** (CCED - Defence Electronic Communications Commissariat), which comes under the Ministry for Electronic Communications. It ensures that electronic-communication requirements are met as they relate to defence and public security, and that operators apply legislative and regulatory requirements in matters of defence and public security;
- **the *Autorité de régulation des communications électroniques et des postes*** (ARCEP – Electronic Communication and Postal Regulatory Authority) is the independent administrative authority tasked with regulating electronic communications in France.

Security strategy

The strategy aims at **avoiding long-term interruption of electronic communications**. Particular attention is paid to malfunctions and to anomalous use of software, because they can be ill-intentioned in origin. In that regard, cybersecurity objectives apply in full to the area of electronic communications.

11.2. Protecting water networks



Description of the area

This area covers all **activities that involve health monitoring and distribution of water to various public and private consumers** in compliance with the rules of the Public Health Code. It includes drinking-water pumping, production, storage, and supply systems.

The permanent health monitoring of *eaux destinées à la consommation humaine* (EDCH – Water for Human Consumption), which guarantees health security, includes health checks implemented by *agences régionales de santé* (ARS – Regional Health Authorities) as well as surveillance

carried out by the *personne responsable de la production ou de la distribution de l'eau* (PRPDE – Person Responsible for the Production and Distribution of Water). Health control is carried out independently of the PRPDEs. It enables checks to be made of compliance with legislative and regulatory provisions relating to the health security of EDCH. Surveillance involves the regular verification of measures taken to protect the resource and the functioning of installations, as well as carrying out analyses at various points.

The production and distribution service that provides drinking water to the population comes under the municipality, the group of municipalities, or the drinking-water supply union (project manager of this public service). Those bodies can either manage the service directly, or delegate its management through a lease contract or a concession contract (based on the degree of delegated authority) granted to a specialist private business.

The public drinking-water service is distinguished by the geographical dispersal across the whole of national territory of over 25,000 drinking-water distribution units (UDI, network part of the physical distribution network that provides high-quality water that is deemed homogenous, of the same origin, having the same owner and the same operator). Those UDIs vary in size (ranging from supplying a few tens of people to several hundreds of thousands of people), and they are rarely interconnected. Not all water distributed is treated.

Security strategy

The strategy aims at **protecting water networks, ensuring that operating those networks receives the requisite level of vigilance, and ensuring continuity of distribution.**

11.3. Protecting electricity networks

Description of the area

This area covers **activities that ensure the continuity of electricity distribution to the population and to all activities**. The area's three main functions are electricity production, transporting electricity across the whole of the territory and in interconnection with other countries, and electricity distribution to all users.

Several actors contribute to protecting the area:

- ◉ the *Commission de régulation de l'énergie* (CRE – Energy Regulation Commission) is the independent administrative authority tasked with overseeing the proper functioning of the electricity and gas markets in France;
- ◉ the State's services issue operating permits based on opinions from the CRE;
- ◉ operators are liable for the continuity of services for which they are responsible: production, transport, or distribution.



Security strategy

The strategy aims at **maintaining the continuity of services by protecting electricity networks** and by ensuring that their operation receives the requisite level of vigilance.

11.4. Protecting hydrocarbon networks

Description of the area

This area covers **the importing, refining, distribution, and delivery of liquid hydrocarbons to various public and private consumers**. All those activities are contained in logistics chains that are interlinked.

Several actors contribute to protecting the area:

- ◉ the State's services (the Direction générale de l'énergie et du climat (DGE – Directorate General for Energy and Climate)) decide on the possible use of strategic stocks as part of agreements linking the Member States of the International Energy Agency, in accordance with European regulations;
- ◉ operators from the oil sector are many and of variable size, and they are distributed according to their more-or-less-integrated logistics activities;
- ◉ large operators acting in integrated activity networks;
- ◉ independent operators that carry out some oil-related activities (distribution and storage);
- ◉ large and medium-sized supermarkets, which have 56% of the market in petrol pumps;
- ◉ distributors of domestic fuel.

The challenges of protecting the area are linked to the very sensitivity of the hydrocarbons stored and transported along networks. Protecting a certain number of infrastructures comes under the plan that covers dangerous installations and materials. Protecting hydrocarbon networks covers, above all, the sensitive components that ensure the functioning and the continuity of transport and distribution services.

Security strategy

The strategy aims at **maintaining the continuity of services by protecting hydrocarbon networks** and by ensuring that their operation receives the requisite level of vigilance.

11.5. Protecting gas networks

Description of the area

This area covers **the transport, storage, and distribution of gas, enabling imports to be used to ensure the continuity of supply to various public and private consumers**, either through an oil pipeline or in the form of liquefied natural gas (LNG) from methane terminals.

Several actors contribute to protecting the area:

- The *Commission de régulation de l'énergie* (CRE) oversees the proper functioning of the gas and electricity markets in France, as well as the independence of administrators;
- the State's services issue operating permits based on opinions from the CRE;
- operators are liable for the continuity of the service for which they are responsible: transport, storage, or distribution.



Security strategy

The strategy aims at **maintaining the continuity of services by protecting gas networks** and by ensuring that their operation receives the requisite level of vigilance.

12. CONTROLLING BORDERS

Description of the area

This area covers **land borders (road and rail), including river and lake borders, maritime borders, and air borders under French sovereignty**. France has 132 points de passage frontaliers (PPF – Border Crossing Points) at external borders, and it has identified at least 285 *points de passage autorisés* (PPA – Authorised Crossing Points) that it can activate at internal borders in case of need.

Implementing VIGIPIRATE border-control measures applies in two contexts:

- ◉ **preventive actions:** some crossing points can be controlled if a national event is organised that requires reinforced protection, or if there is identification of a serious and imminent threat to public order or internal security;
- ◉ **reacting to an attack:** some crossing points can be controlled in the event of a terrorist attack, in order to avoid perpetrators leaving the territory or any accomplices entering the territory.

Several actors contribute to protecting the area:

- ◉ State actors that are responsible for border control: the central directorate of the border police and the directorate general of customs and indirect taxes;
- ◉ State actors intervening as back-up: national *gendarmerie*, national police, armed forces, directorate general of infrastructures, transport, and the sea, regional directorates of the environment, spatial planning, and housing;
- ◉ actors outside the scope of the State: airport and port operators, the European Commission as well as other European States, and the European Border and Coastguard Agency (Frontex).



Security strategy

The security strategy aims at **encouraging interministerial planning and organising the deployment of units engaged in border-control work** as part of the fight against terrorism.

13. PROTECTING FRENCH NATIONALS AND INTERESTS ABROAD

Description of the area

The foreign area of the VIGIPIRATE plan **covers all countries where France has a presence, which host French nationals, and which are likely to receive French travellers.** French presence includes diplomatic and consular missions, military units stationed abroad or on operations, military personnel on co-operation missions, cultural institutes, educational, cultural, and research establishments, and businesses. France ensures that French nationals are protected, whether they are resident or just passing through.

Under the authority of the Prime Minister, the Ministry of Foreign Affairs and International Development defines and implements security measures that apply to diplomatic posts, and provides interministerial co-operation in matters affecting the security of French nationals and interests.

The Ministry of Foreign Affairs has authority over diplomatic missions. The latter are convergence points for all information and ability to take action in the event of a threat abroad. They provide their expertise on each country and provide local liaison with nationals, the network of educational establishments, businesses, local political authorities, and the diplomatic representatives of other countries.

Other ministries are stakeholders in protection abroad. The Ministry of Defence is responsible for defining and implementing protection measures for military units stationed abroad or on operations, as part of agreements signed with host countries. The Ministry of the Interior provides a permanent protection and security mission in a certain number of diplomatic representations. The Ministry of Transport plays a role in protecting air and maritime transport abroad, and liaises with the operators concerned.

Businesses are responsible for the safety of their employees.

The terrorist threat abroad is very varied in its origins and in its manifestations. It can come from organisations or networks that are more or less independent locally or internationally, or even from isolated individuals. It can stem from political and religious ideologies, or from criminal or Mafia-like motivations. It can manifest itself following clearly posted intentions or on an opportunistic basis, based on local political and economic situations and the foreign-policy positions of France and its allies. Modes of action can be greatly varied. Potential targets can be grouped into three main categories: French nationals, missions representing France, and French businesses.

Security strategy

To respond to those challenges abroad, the VIGIPIRATE plan aims at **protecting French residents, vulnerable people, travellers, State employees, aircraft and the aerodromes where they land, and vessels and the ports where they dock.** Moreover, it aims at **reinforcing vigilance around missions representing the State and French businesses.**

FOR MORE INFORMATION

The other PIRATE plans

Plans activated in the event of a terrorist attack that uses a specific means of aggression:

- ◉ the **NRBC plan** (nuclear, radiological, biological, or chemical) sets out the procedures for intervening in the event of a threat or of verified execution of an ill-intentioned action or an action of a terrorist nature using NRBC materials, agents, or products;
- ◉ the **PIRANET plan** enables intervention in the event of an information-technology crisis.

Plans activated in the event of a terrorist attack in a particular setting:

- ◉ the **PIRATAIR-INTRUSAIR plan** is an intervention plan that aims at controlling verified or imminent illicit acts in matters of aviation security (PIRATAIR) and air sovereignty (INTRUSAIR);
- ◉ the **PIRATE-MER plan** enables intervention against maritime terrorism and piracy, and, more generally, against any ill-intentioned act at sea that could be linked to hostage-taking;
- ◉ the **METROPIRATE plan** enables intervention in the event of an attack on underground rail public transport.

Documentation

- ◉ *Interministerial guide for the prevention of radicalisation*, document of the Interministerial committee for the prevention of crime, March 2016
- ◉ *2008 White Paper on defence and national security*, available on line at: <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000341.pdf>
- ◉ *2013 White Paper on defence and national security*, available on line at: <http://www.livreblancdefenseetsecurite.gouv.fr/>
- ◉ *Information leaflet against radicalisation, document of the Ministry of the Interior (MI/SG/DICOM - 04/2015)*, available on: <http://www.interieur.gouv.fr/Sg-CiPDR/Prevenir-la-radicalisation/Prevenir-la-radicalisation>
- ◉ *Decree of 17 December 2015* relating to the use of airspace by aircraft flying with no humans aboard
- ◉ *Decree of 17 December 2015* relating to the design of civil aircraft flying with no humans aboard, their conditions of use, and the skills required of the people using them
- ◉ *9 May 2016 action plan against radicalisation and terrorism*.

Web sites

- ⦿ www.gouvernement.fr
- ⦿ <http://www.risques.gouv.fr>
- ⦿ <http://www.encasdattaque.gouv.fr>
- ⦿ <http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs>
- ⦿ <https://pastel.diplomatie.gouv.fr/fildariane/dyn/protected/accueil/formAccueil.html>
- ⦿ <http://www.service-public.fr/particuliers/vosdroits/F1527>
- ⦿ <http://www.ssi.gouv.fr>

Reporting platforms:

- ⦿ <http://www.stop-djihadisme.gouv.fr/une-question-un-doute.html>
- ⦿ <http://internet-signalement.gouv.fr>

Guides to best practices

- ⦿ *All sectoral guides to VIGIPIRATE best practices can be consulted at:*
<http://www.encasdattaque.gouv.fr>
- ⦿ *Guide to information-technology hygiene aimed at businesses*, available at
<http://www.ssi.gouv.fr/>
- ⦿ *Guide to recommendations for protecting the food chain against the risks of ill-intentioned, criminal, or terrorist actions*, available at
http://agriculture.gouv.fr/sites/minagri/files/documents/pdf/guide-2014_140214_V2

SAIP app

More information at <http://www.gouvernement.fr/appli-alerte-saip>
To download the app, please go to <http://appstore.com>

ANSSI	<i>Agence nationale de la sécurité des systèmes d'information</i> (National Agency for Information-System Security). Attached to the SGDSN, tasked with protection and prevention in the face of cyberthreats. It organises and co-ordinates the implementation of the cybersecurity part of the VIGIPIRATE plan.
ARCEP	<i>Autorité de régulation des communications électroniques et des postes</i> (Electronic Communications and Postal Regulatory Authority) is the independent administrative authority tasked with regulating electronic communications in France.
CCED	The <i>Commissariat aux communications électroniques de défense</i> (Defence Electronic Communications Commissariat) comes under the Ministries of the Economy and Finance. It ensures that communications needs are met in relation to defence and public security.
CIAV	The <i>Cellule interministérielle d'aide aux victimes</i> (Interministerial Cell for Help for Victims) provides real-time centralisation of information on the state of victims. It informs and supports their loved ones, and co-ordinates the work of all intervening ministries, in relation with associations and the prosecution. It comes under the authority of the Prime Minister, who decides when it is activated and when it is closed down.
CNR	<i>Coordonnateur national du renseignement</i> (National Intelligence Co-ordinator), who works beside the President of the Republic. Co-ordinates the work of the intelligence services and ensures that they co-operate appropriately.
CRE	The <i>Commission de régulation de l'énergie</i> (Energy Regulation Commission) is the independent administrative authority tasked with overseeing the proper functioning of the gas and electricity markets in France.
FGTI	The <i>Fonds de garantie</i> (Guarantee Fund) is tasked with compensating victims by way of national solidarity. It carries out recourse actions against the parties responsible for damage.
Frontex	The European Border and Coastguard Agency. Its mission is to co-ordinate operational co-operation between Member States at the external borders of the European Union in matters of the fight against clandestine immigration.
ISPS	The International Ship and Port Facility Security Code.
NRBC	Nuclear, radiological, biological, and chemical. Generic term used to designate unconventional weapons or technological risks of which the effects are difficult to control and contain due to their power or their environmental-dissemination ability.
Security objective	Effect to be obtained in terms of vigilance and protection to counter threats and reduce vulnerabilities in a particular area of activity.

- OIV** Certain operators are described as being of vital importance when their activity sector is one that *“can be substituted and replaced with difficulty in the production of essential goods and services, or can present a serious danger for the population.”* Those services must be essential for satisfying essential needs for the life of populations, exercising State authority, the functioning of the economy, maintaining defence potential, or the security of the Nation.
- Résilience** The 2008 White Paper defines resilience as *“the will and ability of a country, society, and public authorities to resist the consequences of an aggression or a major catastrophe, then swiftly re-establish their ability to function normally, or at least in a socially acceptable manner. It covers not only public authorities but also economic actors and the whole of civil society.”*
- SAIP** *Système d’alerte et d’information des populations* (Population Alert and Information System). Following attacks in France in January and November 2015, and at the Prime Minister’s request, the Ministry of the Interior and the government intelligence service launched a smartphone-based mobile alert app: SAIP, the Population Alert and Information System.
- SAIV** *Sécurité des activités d’importance vitale* (Security of activities of vital importance). A security arrangement that gives a legal framework to operators of vital importance to make them co-operate in protecting their critical installations against any threat, especially of a terrorist nature.
- SIG** *Service d’information du gouvernement* (government intelligence service). A Prime Ministerial department directorate placed under the Prime Minister’s direct authority. It analyses changes in public opinion and media treatment of government action. It informs the general public of the work carried out by the Prime Minister and the government. It steers and co-ordinates government communication at interministerial level.
- SGDSN** *Secrétariat général de la défense et de la sécurité nationale* (Secretariat General for Defence and National Security), a Prime Ministerial department that is tasked, in particular, with steering the VIGIPIRATE plan.
- SHFDS** *Service du haut fonctionnaire de défense et de sécurité* (Department of the Senior Officer of Defence and Security). The Senior Officer is part of the senior civil service. Set beside the Minister, the Senior Officer facilitates and co-ordinates policy in matters of defence, vigilance, crisis prevention, and emergency situations.
- UCLAT** *Unité de coordination de la lutte antiterroriste* (Unit for co-ordinating the fight against terrorism). Placed under the responsibility of the Minister of the Interior, it co-ordinates various departments tasked with the fight against terrorism.

USEFUL NUMBERS

In the event of an attack or to report an abnormal situation¹⁷

112

114 (for persons with hearing or speech difficulties)

In a train or on public transport^{31 17}

or

Text message 31 177

or

Alerte 3117 app

In the event of an attack with a toxic product

15 (SAMU)

18 (firefighters)

112

114 (for persons with hearing or speech difficulties)

Victim of a terrorist attack

15 (SAMU)

08 842 846 37 (7 days a week)

Make a report

Freephone number

0 800 005 696



TACKLING TERRORISM TOGETHER
VIGILANCE, PREVENTION,
AND PROTECTION AGAINST
THE TERRORIST THREAT



51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr