FAIRE FACE ENSEMBLE

VIGILANCE, PRÉVENTION ET PROTECTION FACE À LA MENACE TERRORISTE

Edition décembre 2016

VIGIPIRATE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

SGDSN

*« Nous sommes un peuple libre
qui ne cède à aucune pression,
qui n'a pas peur, parce que nous portons
un idéal qui est plus grand que nous
et que nous sommes capables de le défendre
partout où la paix est menacée. »*

Adresse du Président de la République
à la Nation à la suite des événements
des 7 et 8 janvier 2015 – 9 janvier 2015

PRÉFACE

Depuis le 7 janvier 2015, une vague d'attentats d'une intensité particulièrement dramatique s'est abattue sur notre pays. Si le recours à de tels procédés visant à semer intimidation et effroi n'est malheureusement pas chose nouvelle dans notre histoire, force est néanmoins de constater un changement d'échelle et de nature dans la violence terroriste à laquelle nous sommes confrontés. La brutalité des moyens mis en œuvre atteste de la volonté — au demeurant clairement revendiquée — de tuer en masse et de manière indiscriminée. Le profil des auteurs de ces actes confirme par ailleurs l'existence d'une double menace, à la fois projetée depuis l'étranger et nourrie de l'intérieur via la propagande d'organisations terroristes qui cherchent à retourner contre leur pays nos propres concitoyens.

Pour contrer ce péril terroriste, la France mène une action ferme et résolue. Alors que notre pays continue à s'engager pleinement à l'extérieur, tant sur le plan diplomatique que militaire, notre dispositif de sécurité intérieure a été considérablement durci. Sur le plan juridique, institutionnel et financier, un important effort a été consenti afin d'augmenter et d'améliorer les moyens dont nous disposons, de renforcer la coordination de notre riposte et de cerner l'ensemble des facteurs qui alimentent le phénomène de radicalisation.

Au cœur de cette réponse apportée par les pouvoirs publics, le plan VIGIPIRATE occupe une place particulière. Etabli en 1978, déclenché pour la première fois en 1991 lors de la guerre du Golfe, ce plan constitue un instrument essentiel de vigilance, de prévention et de protection face à la menace terroriste. Conçu pour l'ensemble des acteurs étatiques, il leur propose des mesures opérationnelles et un cadre mobilisateur afin de leur permettre d'anticiper et de répondre à cette menace. Fort de ses quelque 300 mesures, pour partie additionnelles et donc déclenchées uniquement en cas de besoin, il constitue un outil complet qui peut être ajusté avec précision au gré des circonstances.

Pour consolider davantage encore cet instrument et l'adapter à l'évolution de la menace, la réécriture du plan VIGIPIRATE s'avérait néanmoins nécessaire. Elle fut réalisée avec l'ambition de diffuser largement une culture de la sécurité auprès de nos concitoyens. Dans sa nouvelle approche, le plan entend effectivement mieux informer chacun d'entre nous sur le terrorisme, les mécanismes déployés pour y faire face ainsi que sur les gestes et les comportements qui protègent et qui sauvent. Face à une menace diffuse et polymorphe, le devoir de protection reconnu à l'Etat ne doit pas conduire au désengagement du citoyen. Chacun doit, au contraire, s'investir individuellement au profit de la sécurité collective, car chacun est responsable de tous.

Contribuer à cette mobilisation de la Nation contre le terrorisme, telle est l'ambition de ce nouveau plan porté par le Secrétariat général de la défense et de la sécurité nationale.

Louis Gautier
Secrétaire général
de la défense
et de la sécurité nationale

SOMMAIRE

INTRODUCTION

Le plan VIGIPIRATE est au cœur du dispositif national de protection face à la menace terroriste

Au premier rang des menaces retenues dans la stratégie de sécurité nationale[1] figure la menace terroriste, qu'elle s'applique sur le territoire national, contre nos ressortissants ou nos intérêts à l'étranger, ou dans le cyberespace. Pour y faire face, la France dispose d'un dispositif national complet, dans lequel s'insère le plan VIGIPIRATE.

Cet outil d'aide à la décision, mis à la disposition du Premier ministre, associe tous les acteurs nationaux — l'Etat, les collectivités territoriales, les opérateurs publics et privés et les citoyens — à une démarche de **vigilance,** de **prévention** et de **protection.**

VIGIPIRATE : plan national et dispositif global de sécurité

L'Etat doit pouvoir réagir et prendre les mesures nécessaires au cas où la vie de la population ou le fonctionnement régulier de la vie institutionnelle, économique ou sociale du pays seraient mis en cause.

Pour ce faire, **l'Etat dispose d'un ensemble de plans.** Ces documents de planification sont développés au niveau local ou national en prévision de crises de grande ampleur et de catastrophes.

Il existe une vingtaine de plans et autant de déclinaisons spécifiques. Ils se distinguent en deux grandes catégories : **les plans nationaux et les plans territoriaux.**

Elaborés sous l'égide du Secrétariat général de la défense et de la sécurité nationale (SGDSN), **les plans nationaux sont des outils d'aide à la décision pour les plus hautes autorités de l'Etat.** En cas de crise majeure, ils **facilitent la coordination de l'ensemble des acteurs concernés,** au premier rang desquels les différents ministères.

VIGIPIRATE est le seul plan national dont la mise en œuvre est permanente. VIGIPIRATE est donc à la fois un document de planification et un dispositif national de sécurité en évolution constante.

1- Introduite en 2008 par le Livre blanc sur la défense et la sécurité nationale. Voir la rubrique « *En savoir plus* » page 70.

Face à la menace terroriste, un ensemble de plans complémentaires, les **plans de la famille PIRATE,** a été élaboré. **Parmi ces plans antiterroristes, VIGIPIRATE est le seul à être actif en permanence** car il met en œuvre un vaste dispositif de vigilance, de prévention et de protection impliquant un très grand nombre d'acteurs : ministères, forces de sécurité intérieure, opérateurs publics et privés et l'ensemble des citoyens.

Les autres plans de la famille PIRATE sont des plans d'intervention. Ils ont vocation à être activés en cas d'attaque terroriste dans un cadre spécifique comme le milieu aérien, maritime ou le cyberespace ; ce sont les plans NRBC, PIRATAIR-INTRUSAIR, PIRATE-MER, PIRANET, METROPIRATE[2].

Architecture et fonctionnement du plan VIGIPIRATE

Le plan VIGIPIRATE comprend 300 mesures s'appliquant à 13 grands domaines d'action tels que les transports, la santé et les réseaux (détaillés en partie 3). Ces mesures sont réparties entre un socle de mesures permanentes et un ensemble de mesures additionnelles. Ces mesures pouvant être activées en fonction de l'évolution de la menace et des vulnérabilités.

Sur le fondement de l'évaluation de la menace terroriste effectuée par les services de renseignement, **le SGDSN diffuse des directives interministérielles** — les « notes de posture VIGIPIRATE » — **qui déterminent les mesures devant être mises en œuvre** par les acteurs concernés par la vigilance, la prévention et la protection face aux menaces d'action terroriste.

300 mesures
13 domaines d'action

Ces postures sont notamment diffusées :

- à certaines périodes spécifiques de l'année : rentrée scolaire, fêtes de fin d'année, etc. ;
- dans le cadre de grands événements nationaux : célébrations du 70ème anniversaire du débarquement de Normandie, Euro 2016, COP21 ;
- après un attentat, en France ou à l'étranger, pour adapter en urgence le dispositif national de protection.

Cette démarche repose sur trois grands principes :

- l'**analyse croisée de la menace et des vulnérabilités ;**
- une **organisation par domaine d'action** identifiant les leviers qui permettent de réduire les vulnérabilités des grands secteurs du pays en fonction de l'intensité de la menace ;
- une **approche par objectifs de sécurité** permettant de choisir les mesures les plus adaptées et leurs modalités de mise en application.

2- Voir la rubrique « *En savoir plus* » page 70.

La menace terroriste se maintient durablement à un niveau élevé

Le terrorisme

La France, dans son *Livre blanc sur la défense et la sécurité nationale de 2013*, définit le terrorisme comme *« un mode d'action auquel ont recours des adversaires qui s'affranchissent des règles de la guerre conventionnelle »*. Complexe, le terrorisme *« [frappe] les civils sans discernement et la violence [qu'il déploie] vise d'abord à tirer parti des effets que son irruption brutale produit sur les opinions publiques pour contraindre les gouvernements »*.

Défini comme tel, le terrorisme est largement répandu à travers le monde et prend des formes diverses. Son évolution constante le rend particulièrement difficile à appréhender.

Aujourd'hui, un phénomène principalement d'inspiration djihadiste

Le terrorisme est **un phénomène qui a une très longue histoire et il peut être lié à des revendications variées.** Au cours des dernières décennies, des organisations portant des revendications nationalistes ou liées à la décolonisation ainsi que des groupes portant des idéologies extrémistes à fondement politique ou religieux ont commis des attentats sur le territoire national.

Les attentats de 1995 en France ont révélé la nature terroriste de la menace djihadiste qui a pris une échelle mondiale avec le 11 septembre 2001. Portée partout dans le monde à un niveau inédit, elle est notamment incarnée par Al Qaïda, Daech et leurs réseaux affiliés, dont **le projet est d'imposer une idéologie islamiste par la violence.** Depuis 2015, la menace terroriste se maintient durablement à un niveau très élevé en Europe et plus particulièrement en France.

La menace terroriste en France

L'exposition à la menace terroriste des citoyens et des intérêts français, sur le territoire national ou à l'étranger, s'explique notamment par les valeurs et le mode de vie que la République française promeut.

Les attentats qui ont frappé la France en 2015 et 2016 nous ont révélé la nécessité d'intégrer ce phénomène à notre quotidien.

Trois caractéristiques majeures de cette évolution méritent d'être soulignées :

- la **multiplication des types d'acteurs** (personnes radicalisées isolées, équipes opérationnelles déployées en Europe) ;
- la **diversification des modes opératoires** (attaques d'opportunité, attaques planifiées) ;
- la **démultiplication des cibles** (infrastructures, rassemblements, lieux symboliques, etc.).

Les attaques terroristes peuvent également induire des effets d'entraînement et d'imitation. En effet, certains individus aux idées extrêmes, en quête de revanche sociale, de revendication identitaire ou souffrant parfois de troubles psychologiques peuvent être incités à passer à l'acte.

Les modes opératoires utilisés par les terroristes

Dans l'objectif de frapper la France ou ses intérêts, les terroristes recourent à une large panoplie de moyens et à des modes opératoires différents en fonction de leur niveau de préparation.

Les modes opératoires possibles[3] :

- **la fusillade de masse** (avec l'utilisation possible de charges explosives) ;
- **le sur-attentat** consistant, **à la suite d'un premier attentat,** à frapper les secours ou les forces de police ou de gendarmerie arrivés sur place ;
- **l'assassinat de personnalités** (politiques, religieuses, représentants des forces de sécurité, militaires, etc.) ;
- **l'utilisation de voitures, de colis ou de lettres piégés** ;
- **l'utilisation d'agents chimiques toxiques** ;
- **la destruction d'infrastructures symboliques** ;
- **la cyberattaque d'envergure**, compte tenu du développement de l'informatique et du numérique dans notre vie quotidienne ;
- **la prise d'otages** ;
- **la multiplication de fausses alertes à la bombe** ou l'annonce de faux attentats, dans le but d'instaurer un climat de peur.

Les types d'armes utilisées :

Il existe une vaste gamme d'armes utilisées par les terroristes, du simple couteau aux engins explosifs, en passant par les armes par destination (véhicule-bélier, etc.).

3- Cette liste n'est pas exhaustive car les modes opératoires terroristes évoluent et s'adaptent en permanence et ils peuvent être combinés.

PARTIE **1**

LE PLAN VIGIPIRATE

1. LES PRINCIPES ET OBJECTIFS

1.1. Un plan gouvernemental de vigilance, de prévention et de protection

Le plan VIGIPIRATE repose sur trois piliers :

1. la **vigilance** est liée à la connaissance de la menace terroriste et à sa juste prise en compte afin d'ajuster les comportements de chacun et les mesures de protection ;
2. la **prévention** s'appuie sur la sensibilisation des agents de l'Etat, des opérateurs et des citoyens à la menace terroriste, sur leur connaissance de l'organisation du dispositif national et sur la bonne préparation des moyens de protection et de réponse ;
3. enfin, la **protection** repose sur un large éventail de mesures, qui doivent pouvoir s'adapter en permanence à la situation afin de réduire les vulnérabilités sans induire de contraintes disproportionnées sur la vie économique et sociale de la Nation.

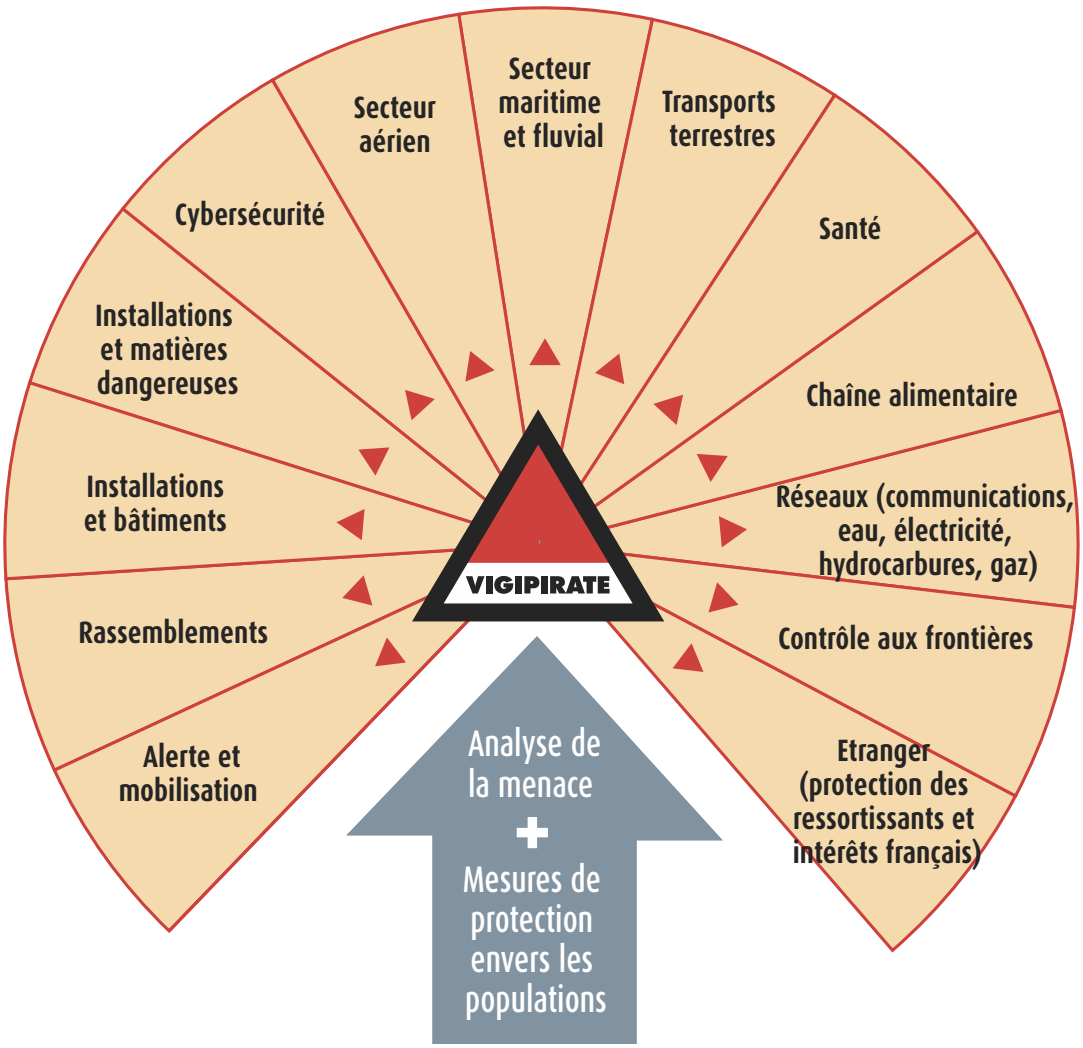
Vigilance
Prévention
Protection

Le plan définit **treize domaines d'action**, soit douze domaines concernant le territoire national et un relatif à l'étranger. Un domaine d'action est constitué par un secteur d'activité ou par une famille de cibles potentielles. Sont décrits au sein des différents domaines d'action :

- les **caractéristiques**, les **enjeux** et les **acteurs** ;
- les **objectifs de sécurité** propres à ce secteur ;
- les **mesures permanentes de vigilance et de protection** à mettre en œuvre en toute circonstance, et qui constituent le socle permanent de vigilance, de prévention et de protection ;
- les **mesures additionnelles** susceptibles d'être mises en œuvre en fonction de l'évaluation de la menace terroriste ou de périodes de vulnérabilités particulières.

Les mesures, qu'elles soient permanentes ou additionnelles, peuvent avoir soit un caractère de recommandation, soit un caractère d'obligation prévu par la loi.

Les 13 domaines d'action du plan VIGIPIRATE



Le plan VIGIPIRATE est prolongé dans certains domaines par des plans d'intervention spécifiques qui mettent en œuvre des moyens spécialisés (plans NRBC, PIRATAIR-INTRUSAIR, PIRATE-MER, PIRANET, METROPIRATE).

1.2. Un plan, des acteurs

Le plan VIGIPIRATE est constitué d'un ensemble de documents qui s'adressent à différents acteurs. Il se décline en une partie publique et une partie classifiée « confidentiel défense ».

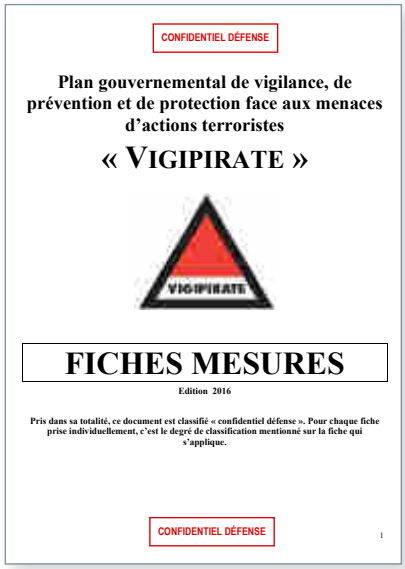
Un document public (le présent document) permet aux entreprises publiques et privées, aux collectivités territoriales, ainsi qu'à chacun des citoyens de comprendre le fonctionnement du plan VIGIPIRATE. **Outil pédagogique et accessible à tous,** la partie publique du plan contribue à **développer une culture de la sécurité collective.**

Certaines informations et modalités de mise en œuvre du plan doivent être protégées et sont donc classifiées, notamment pour ne pas permettre leur exploitation par des adversaires potentiels. La partie « confidentiel défense » du plan VIGIPIRATE comprend deux documents :

- le plan lui-même qui détaille la stratégie, les objectifs et les mesures pour l'ensemble des domaines d'action ;
- une annexe composée de l'ensemble des fiches mesures. Celles-ci sont des fiches réflexes visant à aider la mise en œuvre opérationnelle des mesures et à en préciser le cadre juridique d'application.

Une partie publique :
un document de présentation du plan VIGIPIRATE et de conseils de comportement, destiné à l'ensemble des citoyens et aux professionnels de la sécurité

Une partie « confidentiel défense » : le plan complet destiné aux institutions de l'Etat et à certains opérateurs privés


CONFIDENTIEL DÉFENSE

Plan gouvernemental de vigilance, de prévention et de protection face aux menaces d'actions terroristes

« VIGIPIRATE »

VIGIPIRATE

FICHES MESURES

Edition 2016

Pris dans sa totalité, ce document est classifié « confidentiel défense ». Pour chaque fiche prise individuellement, c'est le degré de classification mentionné sur la fiche qui s'applique.

CONFIDENTIEL DÉFENSE

1

2. LES DIFFÉRENTS ACTEURS DE LA SÉCURITÉ NATIONALE

Outil de mobilisation de l'ensemble de la Nation face à la menace terroriste, le plan VIGIPIRATE associe autour de l'Etat les différentes catégories d'acteurs qui représentent des cibles potentielles pour les terroristes.

2.1. L'Etat

Le **Premier ministre** décide la mise en œuvre des dispositions et des mesures prévues par le plan gouvernemental VIGIPIRATE. Le SGDSN, rattaché directement au Premier ministre, assure le pilotage du plan VIGIPIRATE.

Le **ministre de l'Intérieur,** responsable de la sécurité intérieure, de l'ordre public, de la protection des personnes et de la sauvegarde des installations et des ressources d'intérêt général, veille à la bonne exécution opérationnelle des mesures activées ou mises en œuvre sur l'ensemble du territoire.

Le **ministre des Affaires étrangères et du Développement international** veille à la mise en œuvre des mesures spécifiques lorsque la menace vise des ressortissants, des représentations, des biens ou des intérêts français à l'étranger.

Le **ministre de la Défense** engage les armées dans les milieux terrestre, aérien, maritime et cyber dans le cadre de la manœuvre globale du Gouvernement de lutte antiterroriste sur le territoire national.

Chaque ministre met en œuvre les consignes et les mesures appropriées dans les directions, établissements, services centraux et déconcentrés et les transmet aux opérateurs d'importance vitale, aux services publics, aux grandes entreprises et aux organismes professionnels qui interviennent dans ses champs de compétence.

A l'échelon local, les **préfets de département** — sous la coordination des préfets de zone de défense et de sécurité — veillent à l'information des différents acteurs publics et privés et à la cohérence de la mise en œuvre des mesures dans les territoires, dans le respect de leurs compétences et responsabilités respectives.

2.2. Les collectivités territoriales

Les collectivités territoriales exercent des responsabilités dans de nombreux secteurs de la vie économique et sociale de la Nation. Elles sont concernées à plusieurs titres par la mise en œuvre du plan VIGIPIRATE :

- pour la **protection de leurs installations, de leurs infrastructures et de leurs réseaux** ;
- pour la **continuité des services publics** dont elles ont la responsabilité ;
- pour la **protection de leurs agents** ;
- pour la **sécurité des rassemblements** culturels, sportifs ou festifs qu'elles organisent ou qu'elles accueillent.

Les collectivités territoriales permettent ainsi d'assurer, en liaison avec le préfet, la **continuité territoriale du dispositif général** de vigilance, de prévention et de protection.

2.3. Les entreprises

Certaines entreprises sont désignées « opérateurs d'importance vitale[4] » (OIV) et ont l'obligation légale de mettre en œuvre des mesures de protection spécifiques prévues par la réglementation relative à la sécurité des activités d'importance vitale, mais aussi par le plan VIGIPIRATE.

D'une manière générale, toutes les entreprises publiques et privées doivent **veiller à leur propre sécurité** et, éventuellement, à celle des **personnes qu'elles accueillent**. Elles mettent en œuvre les mesures adaptées dans la limite des prérogatives que la loi leur accorde.

2.4. L'ensemble des citoyens

Par son comportement responsable, tout citoyen contribue à la vigilance, à la prévention et à la protection de la collectivité contre les menaces terroristes. Le plan public VIGIPIRATE familiarise les citoyens avec les comportements à adopter dans le contexte d'une menace terroriste.

2.5. Les acteurs à l'étranger

A l'étranger, la sécurité de l'ensemble des ressortissants français est, **en premier lieu, à la charge de l'Etat où ils se trouvent.** Néanmoins, tout opérateur ou **toute entreprise a l'obligation d'assurer la sécurité de ses employés.**

Le ministère des Affaires étrangères et du Développement international transmet ses instructions à l'ensemble des missions diplomatiques, lesquelles s'en font les relais auprès de la communauté française, des employeurs, des médias locaux et des Etats hôtes.

4- Voir la rubrique « *Glossaire* » page 73.

3. UN DISPOSITIF DE SÉCURITÉ EN ADAPTATION PERMANENTE

Le plan VIGIPIRATE permet d'adapter en permanence le dispositif de vigilance, de prévention et de protection face aux menaces d'actions terroristes. Pour ce faire, des directives appelées « postures VIGIPIRATE » sont régulièrement diffusées par toute la chaîne ministérielle et préfectorale.

Ces postures sont préparées par le SGDSN, en étroite coordination avec les services de l'ensemble des ministères. Elles sont diffusées à certains moments spécifiques de l'année (rentrée scolaire, fêtes de fin d'année, période estivale, etc.), dans le cadre de la préparation des grands événements nationaux (70ème anniversaire du débarquement en Normandie en 2014, COP21 en 2016, Euro 2016, etc.) ou après un attentat.

La mise en œuvre du plan VIGIPIRATE combine trois démarches :

1. **évaluer la menace** terroriste en France et à l'encontre des ressortissants et intérêts français à l'étranger ;
2. **connaître les vulnérabilités des principales cibles potentielles** d'attaque terroriste afin de les réduire et de limiter préventivement les effets d'une telle attaque ;
3. **déterminer un dispositif de sécurité** répondant au niveau de risque qui résulte du croisement des vulnérabilités avec l'état de la menace.

3.1. Evaluer la menace

L'évaluation de la menace terroriste est assurée par un groupe de travail spécifique rassemblant tous les services de renseignement, mandaté et animé par le coordonnateur national du renseignement.

Il fournit une évaluation de façon régulière, en fonction de l'actualité. Peuvent s'y ajouter des évaluations thématiques, appliquées à des secteurs ou à des domaines d'activités ou à des sujets d'intérêt particulier.

Ces analyses sont utilisées afin de préparer les notes de postures VIGIPIRATE.

3.2. Connaître les vulnérabilités des cibles afin de les réduire

Le plan définit **treize domaines d'action**[5], soit douze domaines concernant le territoire national et un relatif à l'étranger. Un domaine d'action est constitué par un secteur d'activité ou par une famille de cibles potentielles, ce qui permet de définir une stratégie de réponse cohérente.

Ainsi, pour chaque domaine d'action est décrite une stratégie qui détaille les vulnérabilités du milieu concerné et définit les objectifs de sécurité à mettre en œuvre pour réduire leurs fragilités face à la menace.

5- Voir la liste des domaines en page 13 et la partie 3 *« Domaines d'action »*.

Chaque objectif de sécurité s'appuie sur des mesures opérationnelles, classées en fonction du degré de contrainte que leur mise en œuvre implique. Deux types de mesures sont distingués :

- les **mesures permanentes** (ou **mesures socles**), qui constituent la posture permanente de sécurité ;
- les **mesures additionnelles,** dont quelques-unes peuvent être très contraignantes, qui sont mises en œuvre de façon circonstanciée et limitée dans le temps, pour faire face à l'aggravation de la menace et/ou des vulnérabilités.

Certaines mesures, qu'elles soient permanentes ou additionnelles, ont un caractère obligatoire.

Les autres mesures relèvent des bonnes pratiques en matière de sécurité, dont la mise en œuvre est recommandée par le plan VIGIPIRATE. Elles font l'objet d'une communication adaptée visant à inciter les acteurs concernés à les appliquer.

La plupart des mesures sont rendues publiques afin d'en faciliter la diffusion. Seules quelques mesures additionnelles sont confidentielles car leur publication pourrait faciliter l'action terroriste.

Les conditions de mise en œuvre des mesures — dans le domaine juridique notamment — sont détaillées dans des fiches d'aide à la mise en œuvre, dénommées ***fiches mesures***, annexées au plan « confidentiel défense ».

3.3. Adapter la posture VIGIPIRATE

La posture VIGIPIRATE est une directive interministérielle, décidée par le Premier ministre, qui adapte le dispositif de vigilance, de prévention et de protection. Elle **comprend le niveau VIGIPIRATE, les objectifs de sécurité retenus, les mesures actives ainsi que des éléments de communication gouvernementale.** Elle précise les mesures socles et mentionne les mesures additionnelles décidées avec, éventuellement, des précisions sur leur cadre et leurs modalités d'application, ainsi que la durée de leur mise en œuvre.

Elle est traduite dans un document confidentiel qui comporte également l'évaluation de la menace terroriste. Elle est validée par le Premier ministre et diffusée par le SGDSN. Cette posture est déclinée par chaque ministère au travers de directives spécifiques.

3.3.1. Le niveau VIGIPIRATE

Le niveau VIGIPIRATE est rendu public. Il est destiné à **signifier la vigilance de la Nation face à la menace terroriste et, en cas de nécessité, la mise en alerte du pays** face à une situation de menace avérée ou d'attentat réalisé. Il ne concerne que le territoire national et les DOM-COM.

Il est décidé par le Premier ministre à la suite de l'évaluation du risque terroriste réalisée par le croisement de la menace et des vulnérabilités.

Le dispositif choisi doit être strictement dimensionné à l'évaluation de la menace.

Trois niveaux sont distingués :
« vigilance », « sécurité renforcée-risque attentat » et « urgence attentat ».

Niveaux	Principes d'activation du niveau	Conditions de mise en œuvre	Types de mesures activées
Vigilance 	Ce niveau correspond à la posture permanente de sécurité.	Ce niveau est valable en tout lieu et en tout temps.	Mise en œuvre de la totalité des mesures permanentes (socle).
Sécurité renforcée-risque attentat 	Ce niveau traduit la réponse de l'Etat à un niveau élevé de la menace terroriste.	Ce niveau peut concerner l'ensemble du territoire national ou être ciblé sur une zone géographique ou un secteur d'activité particulier. Ce niveau n'a pas de limite de temps définie.	Renforcement des mesures permanentes et activation de mesures additionnelles.
Urgence attentat 	Ce niveau déclenche un état de vigilance et de protection maximal, soit en cas de menace d'attaque terroriste documentée et imminente[6], soit à la suite immédiate d'un attentat. L'activation de ce niveau permet d'adapter le dispositif de protection pour prévenir tout risque de sur-attentat.	Ce niveau peut être activé sur l'ensemble du territoire national ou sur une zone géographique délimitée. Par nature de courte durée, le niveau « urgence attentat » peut être désactivé dès la fin de la gestion de crise.	Renforcement des mesures permanentes et activation de mesures additionnelles. Ce niveau est associé à des mesures additionnelles contraignantes et à un renforcement de l'alerte qui peut être couplé à la diffusion d'informations via l'application téléphonique SAIP[7], les différents sites Internet institutionnels, la télévision ou encore la radio. Des conseils comportementaux peuvent également être diffusés à la population en cas de risque de sur-attentat.

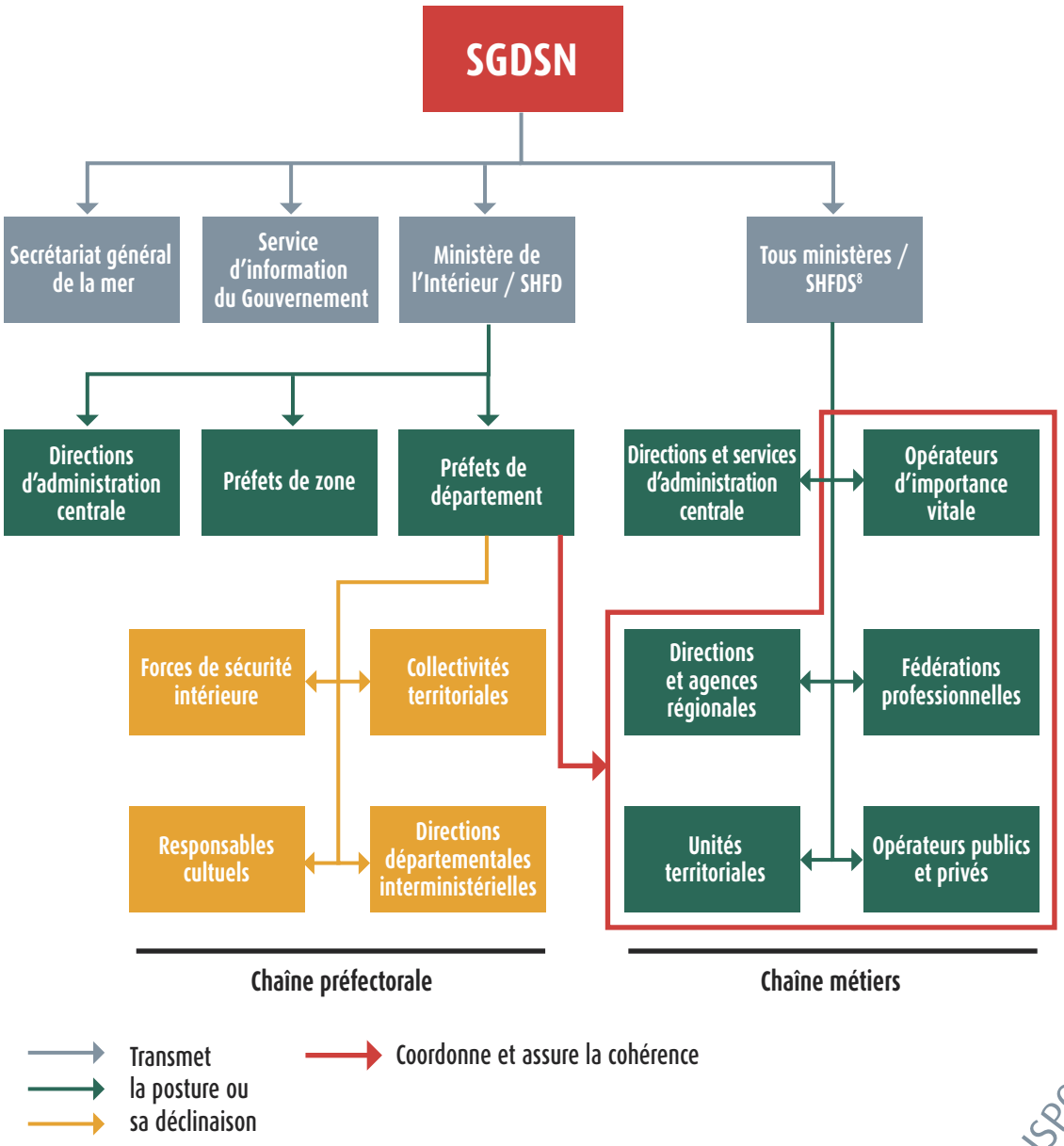
6- La définition de l'imminence reste subjective. L'objectiver revient, sur la base d'informations issues de la communauté du renseignement, à répondre avec précision à au moins deux des quatre questions : qui ? où ? quand ? et comment ?

7- SAIP : Système d'alerte et d'information des populations (application pour smartphone), voir « *En savoir plus* » page 71 et « *Glossaire* » page 73.

3.3.2. Diffusion des instructions de posture VIGIPIRATE

Conformément aux instructions données par le Premier ministre, chaque ministère donne des instructions dans son champ de compétence propre. Le ministère de l'Intérieur joue un rôle prépondérant sur le territoire national par l'intermédiaire des préfets, de la police nationale, de la gendarmerie nationale et de la sécurité civile. Les mesures sont mises en œuvre par une grande diversité d'acteurs : les acteurs étatiques (administrations, services déconcentrés), les collectivités territoriales, les entreprises publiques et privées, les fédérations professionnelles, etc. Les citoyens sont aussi appelés à être acteurs de certaines mesures de vigilance simples.

Circuit de diffusion des notes et instructions de posture VIGIPIRATE



8- SHFDS : Service du haut fonctionnaire de défense et de sécurité.

▶ PARTIE **2**

TOUS IMPLIQUÉS

1. SE PRÉPARER

1.1. Citoyen, que puis-je faire ?

1.1.1. Pourquoi être un citoyen attentif ?

Les terroristes agissent la plupart du temps en vue d'un objectif politique, identitaire ou idéologique. Pour l'atteindre, ils cherchent à briser l'unité des sociétés qu'ils attaquent en fracturant les liens fondamentaux qui les composent.

Si le souci de la sécurité doit nous conduire à renforcer notre vigilance collective, nous ne devons pas pour autant nous méfier de tout le monde. La vraie résilience de la Nation repose sur l'adhésion de tous les citoyens à des valeurs communes et non sur l'éviction de quelques-uns.

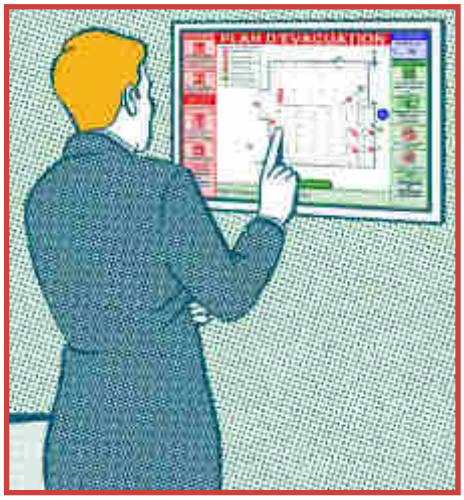
Etre attentif c'est :

- continuer à porter, sur les autres, un regard ouvert et non de crainte ;
- agir pour la sécurité de tous en signalant toute situation ou tout comportement à risque ;
- prévenir le basculement vers un comportement criminel d'un individu en le signalant, avec le souci de protéger la population mais également l'individu en question contre lui-même ;
- veiller à ce que notre propre comportement ne mette pas en danger la sécurité des autres (fausse rumeur, etc.) et qu'il n'entretienne pas un climat de peur.

Etre attentif aux autres et à son environnement

1.1.2. Comment être un citoyen attentif ?

Bien connaître son environnement quotidien :



- connaissez la configuration des lieux de vie et des sites que vous fréquentez habituellement : bâtiment, rue, quartier, agencement des bâtiments, aménagement des espaces, cheminements et issues de secours ;
- sachez auprès de qui signaler les comportements et situations inhabituels ;
- prenez l'habitude d'observer votre environnement avec attention et notamment lorsque vous vous trouvez dans des lieux de forte affluence (gares, transports collectifs, grands rassemblements, etc.).

Se préparer et anticiper les situations d'urgence :

- fiez-vous à votre intuition ;
- préparez-vous à vivre une situation potentiellement violente :
  - envisagez dans chaque endroit où vous vous trouvez la réaction la plus appropriée en cas d'attaque ;
  - identifiez les sorties de secours ;
  - établissez un cheminement d'évacuation dans tout lieu fermé ou de rassemblement important (cinémas, piscines, centres commerciaux, etc.) ;
- gardez toujours sur vous les numéros d'urgence ;
- téléchargez l'application SAIP sur votre smartphone[9].

Avoir un comportement responsable :

- veillez à ce que votre attitude ou votre comportement ne laisse pas penser que vos intentions puissent être malveillantes (masque du visage avec un casque de moto à l'intérieur d'un bâtiment public, utilisation d'armes factices ou de déguisements en tenue paramilitaire sur la voie publique, fausse alerte à la bombe, menaces verbales à caractère terroriste, etc.) ;
- ne prenez pas de photos aux abords des sites qui l'interdisent ;
- conformez-vous aux recommandations, instructions et consignes des pouvoirs publics, forces de l'ordre et des agents de sécurité (inspections des sacs, paquets, bagages à main, palpations de sécurité, respect des périmètres de sécurité) ;
- ne signalez pas les dispositifs de contrôle mis en place par les forces de l'ordre (appels de phares sur la route pour signaler un barrage routier, etc.) ;
- ne vous faites pas le relais de fausses rumeurs ;
- ne laissez pas d'effets personnels (sacs, bagages) sans surveillance ;
- lors des déplacements, n'acceptez pas de prendre en charge un bagage, un objet ou un colis d'un inconnu.

9- Voir « *En savoir plus* » page 71.

Se former aux gestes de premiers secours :

- alerter les secours, procéder à un massage cardiaque, traiter les hémorragies sont les gestes essentiels d'urgence qui peuvent être pratiqués lors de situations d'une gravité exceptionnelle. Ces gestes essentiels peuvent sauver des vies ;
- nombre d'associations agréées de sécurité civile assurent des actions d'enseignement et de formation au secourisme. L'agrément est délivré, après vérification des compétences des associations ;
- si vous souhaitez vous former aux premiers secours, consultez la liste des associations agréées à la formation des gestes de premiers secours[10].

Préparer ses voyages à l'étranger :

Avant chaque voyage à l'étranger :

- consultez le site **http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs** pour prendre connaissance des conseils qui sont régulièrement actualisés ;
- inscrivez votre séjour sur le portail Ariane **https://pastel.diplomatie.gouv.fr/fildariane/dyn/protected/accueil/formAccueil.html** afin de recevoir les messages d'alerte éventuels ;
- dans le cas d'une expatriation (séjour de plus de 6 mois), les ressortissants français et leurs familles doivent s'inscrire sur le registre des Français établis à l'étranger, auprès du consulat de France compétent.

1.1.3. La cybervigilance

Avoir les bons réflexes sur Internet :

La vie des entreprises, des administrations et de nos concitoyens est dorénavant dépendante du numérique et des moyens informatiques utilisés au quotidien. Ces outils peuvent être un puissant vecteur pour les terroristes qui souhaitent atteindre la société dans son ensemble. Pour cette raison, il est essentiel de se protéger en acquérant des réflexes simples.

- protégez vos informations personnelles, professionnelles et votre identité numérique ;
- cliquez toujours avec discernement sur les liens et les pièces jointes ;
- choisissez des mots de passe élaborés pour chaque compte ;
- gardez vos mots de passe à l'abri et ne les communiquez à personne ;
- ne révélez jamais votre numéro de carte de paiement par mail ;
- effectuez vos paiements sur des sites sécurisés ;
- protégez vos données lors de vos déplacements ;
- privilégiez les accès WIFI sécurisés et les supports amovibles personnels (clés USB) ;
- mettez à jour régulièrement les logiciels installés sur vos ordinateurs, ordiphones et tablettes, notamment votre antivirus ;
- désactivez les interfaces sans fil lorsqu'elles ne sont pas nécessaires ;

10- Consultez la liste des associations agréées : http://www.gouvernement.fr/risques/se-former-aux-premiers-secours

- effectuez des sauvegardes régulières ;
- pensez à sécuriser votre box Internet ;
- signalez les sites Internet et les réseaux sociaux suspects ou faisant l'apologie du terrorisme[11].

Retrouvez les recommandations et bonnes pratiques sur le site de l'ANSSI :

- pour les administrations : **http://ssi.gouv.fr/administration/bonnes-pratiques**
- pour les entreprises : **http://ssi.gouv.fr/entreprise/precautions-elementaires**
- pour les particuliers : **http://ssi.gouv.fr/particulier/precautions-elementaires**
- pour tous : le site **http://www.risques.gouv.fr**

Savoir protéger son identité et ses informations personnelles :

Sur Internet, les occasions de partager des moments de sa vie privée sont nombreuses. Si la multiplication des réseaux sociaux vous permet de rester en relation avec votre famille et vos amis, ces réseaux ne sont pas sans risque pour votre sécurité. Aussi, lorsque vous les utilisez, gardez à l'esprit qu'une personne malintentionnée pourrait utiliser à des fins criminelles les informations personnelles que vous publiez.

Lorsque vous exercez un métier qui pourrait constituer une cible pour un terroriste, **il est fortement recommandé de ne pas divulguer d'informations sur votre domicile ou vos habitudes,** de toujours penser à l'utilisation qui pourrait être faite de vos données et de préserver autant que possible la confidentialité de votre vie privée.

Votre identité numérique est précieuse et les traces que vous laissez en publiant vos informations personnelles demeureront accessibles quasi indéfiniment.

Les terroristes utilisent les données présentes sur Internet pour mieux connaître et atteindre leurs cibles

Par conséquent, protégez-vous et protégez vos proches en restant prudent sur ce que vous publiez sur Internet.

11- Signalez sur le site https://www.internet-signalement.gouv.fr/

1.2. Directeurs et responsables de sites accueillant du public, comment vous préparer ?

Tout responsable d'établissement recevant du public est encouragé à décliner VIGIPIRATE dans son propre plan de sûreté d'entreprise. Ce plan prévoit les mesures à prendre en cas de menace ou d'attentat, ou simplement de risques tels que la découverte d'objets abandonnés.

Il fixe les dispositions spéciales à appliquer en matière de surveillance, d'organisation et de contrôle. Chaque agent de la société est informé de ce qu'il doit faire dans le cadre du plan d'entreprise.

L'Etat encourage particulièrement les établissements recevant du public à **établir des procédures de réaction en cas d'attaque terroriste et à sensibiliser leurs employés.**

A cette fin, les autorités ont préparé, en liaison avec les acteurs concernés, un ensemble de **guides de bonnes pratiques**[12] à destination des responsables d'établissements recevant du public, qui présentent les comportements individuels et collectifs à adopter pour se préparer à une attaque terroriste.

Une bonne organisation préalable de vos établissements ainsi qu'une réaction adaptée des personnels peuvent sauver des vies.

1.2.1. Préparer son organisation à un acte de malveillance ou de terrorisme

De nombreux conseils sont délivrés ci-dessous. Certains peuvent être difficilement applicables par l'ensemble des sites. Ils doivent donc être adaptés en fonction de la situation.

a) Développer les relations avec les partenaires extérieurs

Les différents partenaires extérieurs :

- **le préfet et les services préfectoraux.** Ils évaluent le niveau de la menace et établissent les mesures de vigilance et de protection à adopter dans le cadre de la mise en œuvre du plan VIGIPIRATE ;
- **le maire et les services municipaux.** Ils complètent l'action des forces de police et de gendarmerie. Ils procèdent aux aménagement de voie publique nécessaires à la protection des installations exposées ;
- **les forces de police et de gendarmerie.** Elles peuvent, en s'appuyant sur leurs référents sûreté, apporter des conseils de sécurité aux responsables de site sur le renforcement de leurs mesures de sécurité. Des rencontres régulières avec les forces de police et de gendarmerie participent de la connaissance mutuelle. Pour les sites représentant une sensibilité particulière, des plans des bâtiments peuvent être remis aux forces de sécurité afin de faciliter une intervention en cas d'attaque.

12- Voir les guides sectoriels de bonnes pratiques sur http://www.gouvernement.fr/reagir-attaque-terroriste

b) Analyser les vulnérabilités de son établissement

- identifiez en quoi votre établissement pourrait être une cible (lieu de grands rassemblements de personnes, site représentant les institutions du pays, site symbolique du mode de vie occidental ou des valeurs de la République française, lieu de culte, etc.) ;
- identifiez ce qui pourrait être ciblé dans votre établissement : personnels, infrastructures, informations, produits ou matériels spécifiques qui pourraient être volés en vue d'une action terroriste ;
- identifiez les vulnérabilités physiques de l'établissement (nombre d'accès, portes ne fermant pas à clef, accès livraison non surveillés, etc.) ;
- envisagez les moyens d'action possibles (arme blanche, arme automatique, voiture-bélier, colis ou véhicule piégé) ;
- prenez en compte la menace interne (radicalisation pouvant devenir violente par exemple).

c) S'organiser

Renforcer la protection du site :

- limitez le nombre d'accès pour une meilleure surveillance des flux sans réduire la capacité d'évacuation de vos employés et du public ;
- déployez un système de vidéo-protection ;
- mettez en place un système de badges d'accès ;
- installez un système d'interphone, si possible avec caméra ;
- faites en sorte que les portes d'accès au site soient éclairées ;
- changez régulièrement les codes des claviers alphanumériques de type Digicode ;
- mettez en place un système de filtrage et de fouille aux accès ;
- protégez l'accès extérieur du site de toute possibilité d'attaque d'un véhicule-bélier (mise en place de plots, bacs de fleurs, blocs de béton, herses mobiles, etc.) ;
- coordonnez-vous avec les établissements ou les entreprises limitrophes ;
- faites en sorte que les parties communes et les zones techniques du site soient maintenues propres et qu'on ne puisse pas y dissimuler de colis abandonnés ;
- vérifiez la disponibilité des issues de secours.

Mettre en place des moyens d'alerte spécifiques :

- *Alerter au sein de l'organisation.* **Il est essentiel que chaque organisation puisse donner l'alerte en cas d'attaque terroriste**. Le système d'alerte conditionne la réaction de l'ensemble des personnes occupant le site et doit être distinct de l'alarme incendie car la réaction attendue n'est pas la même. Un tel système ne s'improvise pas et il est recommandé de l'établir en concertation avec le personnel de l'établissement. Ces moyens d'alerte doivent être connus de tous et testés régulièrement à l'occasion de mises en situation et d'exercices.
- Pour que la procédure d'alerte soit complète, il faut mettre en place deux systèmes :
  - **un système d'alerte décentralisé** qui permette à chacun de donner l'alerte une fois l'acte de malveillance constaté (sifflet, téléphone fixe, SMS téléphonique, système de bipeur, radio, etc.) ;
  - **un système d'alerte centralisé** qui permette de prévenir l'ensemble du site (surtout s'il est étendu) : alarme sonore distincte de l'alarme incendie, message par haut-parleur, avertisseur lumineux, SMS téléphonique, corne de brume, etc.

- **L'alerte a pour vocation de prévenir d'une attaque.** Idéalement, deux types d'attaques doivent être distingués car ils n'appellent pas les mêmes réactions :
  - l'attaque extérieure au site et à proximité (confinement recommandé) ;
  - l'attaque dans le site (évacuation ou confinement en fonction de la localisation des personnes dans le bâtiment). **Il n'est pas recommandé d'imposer une réaction unique pour l'ensemble du site concerné, en cas d'attaque interne.** Certaines personnes peuvent facilement s'échapper du fait de la situation de leurs locaux, d'autres ne peuvent pas fuir facilement et doivent donc se confiner. Il est, par conséquent, préférable de laisser l'initiative aux personnes occupant le site.

Pour distinguer les deux types d'attaques (interne et externe), des codes sonores ou visuels différents peuvent être employés. Par exemple, une attaque extérieure pourra être signalée par 3 longues sonneries alors qu'une attaque sur le site pourra être signalée par 6 longues sonneries. De même, si l'alerte est donnée par SMS, le message doit préciser si l'attaque est interne ou externe au site.

- *Alerter hors de l'organisation :* forces de sécurité, établissements extérieurs sensibles (hôpitaux, écoles, etc.). **Plus vite l'alerte est donnée et plus vite les forces de sécurité intérieure peuvent intervenir.**
- Sensibilisez vos employés au fait que chacun doit se sentir responsable et doit prévenir en cas d'attaque. Le message à faire passer est le suivant : **« ne pensez pas que d'autres ont donné l'alerte, faites-le ».**

Préparer :

- une **mallette de crise** avec les numéros de téléphone des personnes à joindre et les plans du site qui pourraient être remis aux forces de sécurité en cas d'attaque ;
- des **procédures de réaction adaptées** aux différents actes de malveillance :
  - alerte à la bombe (privilégier la même réaction qu'une alerte incendie) ;
  - attaque à l'intérieur du site (évacuation ou confinement) ;
  - attaque à l'extérieur mais à proximité du site (confinement privilégié) ;
- des **itinéraires d'évacuation** (ce ne sont pas forcément les issues de secours, un toit peut faire office de protection par exemple) ;
- des **pièces de confinement** connues de tous. Les fermetures des portes peuvent être renforcées à moindre coût.

Sensibiliser le personnel :

Informer le personnel :

- informez les agents sur la menace et sur les différentes bonnes pratiques à avoir dans un contexte de menace terroriste ;
- **développez une stratégie de sensibilisation interne** en apposant l'affiche (*voir page 43*) et en diffusant la vidéo « Réagir en cas d'attaque terroriste »[13]. Les guides de bonnes pratiques propres à certains secteurs professionnels peuvent également être distribués ;
- sensibilisez le personnel au respect des mesures de sécurité et de vigilance ;
- **rappelez les procédures et le rôle de chacun ;**
  - informez les agents sur la procédure de signalement de comportements suspects (employé manifestant une pensée extrême, potentiellement violente) ;
  - encouragez la vigilance des employés afin de détecter et de signaler les comportements suspects.

13- Voir le site http://www.gouvernement.fr/reagir-attaque-terroriste

Former le personnel :

- encouragez la formation aux premiers secours ;
- assurez-vous de la connaissance et de la maîtrise par tous des moyens d'alerte ;
- favorisez la connaissance du site en organisant des « reconnaissances exploratoires » afin d'identifier les cheminements, les issues de secours, les obstacles éventuels, et tout ce qui peut offrir une protection ;
- organisez des mises en situation simples et des exercices collectifs, intégrant éventuellement les différents partenaires, et en exploitant systématiquement les retours d'expérience de ces exercices.

1.2.2. Préparer un rassemblement[14]

La sécurité d'un événement ne s'improvise pas. Faites-vous conseiller par des professionnels. Pour se préparer à un rassemblement de personnes, il faut :

a) Identifier les menaces et les vulnérabilités

Evaluer la sensibilité du rassemblement en lien avec les services de l'Etat. Pourquoi ce rassemblement pourrait-il être ciblé par des terroristes ? En quoi est-il un symbole du mode de vie occidental et des valeurs de la République ? Ce rassemblement a-t-il une couverture médiatique qui donnerait une forte visibilité à une action terroriste ?

Envisager les différentes attaques possibles : jet ou dépôt d'un engin explosif, véhicule piégé en stationnement aux abords du site, véhicule-bélier, fusillade, attaque à l'arme blanche, etc.

Mettre en place des partenariats avec les acteurs publics locaux :

- **organisez** les relations avec les autorités de police administrative (préfet et maire) afin d'évaluer la menace et les mesures de vigilance et de protection à adopter dans le cadre du rassemblement ;
- **coordonnez-vous** avec les forces de police, gendarmerie, police municipale ou les sapeurs-pompiers.

Si les obligations de sécurité du public ne peuvent être satisfaites ou si les circonstances l'exigent, l'organisateur peut renoncer à la manifestation.

14- Voir également la fiche 2 page 55.

b) Organiser la sécurité de l'événement

La périphérie :

- interdire le stationnement de tout véhicule aux abords immédiats du lieu du rassemblement ;
- mettre en place une signalétique afin d'orienter les piétons sur le lieu de l'événement et de détourner les flux de véhicules ;
- identifier le mobilier urbain qui pourrait servir à dissimuler de l'explosif, l'enlever, en réduire l'utilisation ou mettre en place des rondes de vérification ;
- solliciter les forces de l'ordre ou la police municipale pour la réalisation de patrouilles, voire la mise en place de points de contrôle et de filtrage ;
- identifier les points de vulnérabilité hauts (immeubles surplombants) et les sécuriser, éventuellement par une présence humaine ;
- si possible, mettre en place un système de vidéo-protection donnant, en priorité, sur les accès au site.

La périmétrie :

- installer une délimitation physique de l'événement au moyen de barrières reliées entre elles ;
- organiser un cheminement jusqu'au point de contrôle en installant des barrières ;
- séparer les flux entrants et les flux sortants ;
- aménager, au niveau des accès, des points de contrôle tenus par des agents de sécurité en nombre suffisant afin de fluidifier le plus possible l'entrée du public (l'utilisation de magnétomètres ou de portiques détecteurs de masses métalliques permet d'accroître la qualité des filtrages) ;
- sensibiliser les agents privés de sécurité (consignes de vigilance, etc.) et rappeler par des briefings quotidiens les réactions à adopter en cas d'événement suspect, d'acte de malveillance ou d'attaque terroriste. Les procédures de remontée d'alarme doivent être connues et maîtrisées de tous ;
- doter les agents de sécurité de moyens radio ;
- installer, au niveau des accès publics (entrées et sorties) des dispositifs (blocs de béton, etc.) visant à entraver toute intrusion de véhicule-bélier ;
- contrôler par une présence humaine les points de sortie afin qu'ils ne permettent pas d'intrusion ;
- aménager les issues de secours en nombre suffisant au regard de l'importance de l'événement afin de permettre une évacuation rapide du public en cas de danger à l'intérieur de la zone.

Les volumes intérieurs :

- désigner un responsable sûreté qui sera l'interlocuteur unique des forces de police et de gendarmerie et des secours en cas d'intervention sur le site ;
- faire appel aux compétences de sociétés privées de sécurité pour assurer la sécurité d'un tel événement ;
- sécuriser la zone en période de fermeture au public par la mise en œuvre d'un gardiennage humain ;
- prévoir l'aménagement d'un poste central de sûreté au cœur du site. Ce dernier doit être équipé 24 heures/24 par au moins un opérateur qui visualisera les images du système de vidéo-protection mis en place ;
- sensibiliser les collaborateurs et exposants aux niveaux de menace, aux modes opératoires terroristes et à la détection d'actions de repérage. Cette sensibilisation doit être complétée par une information sur les comportements à adopter en cas d'attaque ;
- installer des écrans et des haut-parleurs pouvant diffuser une alerte (pré-enregistrée si possible) ;
- organiser et contrôler les livraisons.

1.2.3. Réaliser des exercices progressifs

Les exercices de réaction à une attaque armée doivent être progressifs et doivent toujours donner lieu à un retour d'expérience collectif qui permette d'en tirer les enseignements et d'en améliorer les procédures.

Types d'exercices :

1. **rappel simple des procédures** et du rôle de chacun par le responsable du site ou son chargé de sûreté ;
2. **exercice « sur table »** au cours duquel, dans une salle, les employés présentent la réaction qu'ils auraient en cas d'attaque. La séance doit être scénarisée (lieu, nombre et armes des assaillants identifiés) ;
3. **test technique du système d'alerte ;**
4. **organisation de reconnaissances exploratoires** (lieux d'évacuation, salles de confinement, etc.) ;
5. **exercice de mise en situation avec des personnes simulant l'intrusion.** Les employés doivent être prévenus de la réalisation de l'exercice mais pas nécessairement de sa date exacte. Pour éviter tout phénomène de panique, il faut établir un moyen de faire comprendre à tous qu'il s'agit d'un exercice. **Les forces de police et de gendarmerie doivent impérativement être informées de la réalisation de ce type d'exercice** et peuvent y être invitées pour apporter leur expertise. Pour réussir un tel exercice, il faut déterminer clairement à l'avance les objectifs à atteindre et élaborer une méthode rigoureuse d'évaluation. Cette dernière est essentielle pour en tirer de bons enseignements et doit s'appuyer sur une équipe d'évaluateurs qui observent le déroulement de l'ensemble de l'exercice.

2. PRÉVENIR

2.1. Prévention et signalement des cas de radicalisation

La radicalisation se caractérise par un « **changement de comportement qui peut conduire certaines personnes à l'extrémisme ou au terrorisme** »[15].

a) Pourquoi signaler un cas de radicalisation ?

La radicalisation **concerne tout type d'idéologie** qui peut conduire l'individu à choisir l'action violente au nom de convictions auxquelles il adhère **sans compromis possible.** Cette action violente peut causer la mort d'autres membres de la société dont il rejette inconditionnellement les valeurs et le mode de vie.

On parle ainsi de **processus de radicalisation** par paliers avec adhésion à une idéologie et rupture avec l'environnement habituel. La radicalisation apparaît comme un phénomène profondément lié à l'exploitation de conflits d'identité, de frustrations ou de fragilités. Certains groupes terroristes cherchent notamment à enrôler des individus en perte de repères et vulnérables.

La force d'une idéologie et son pouvoir d'attraction ne doivent pas être sous-estimés. Des individus ayant développé une haine de notre société peuvent adhérer pleinement à un discours qui donne sens à leurs frustrations ou sentiment d'humiliation.

La radicalisation est un phénomène complexe, amplifié par le développement des réseaux sociaux. La propagande véhiculée par des individus ou par des groupes touche des profils variés : délinquants, personnes vulnérables en quête d'identité, personnes ayant des troubles psychiatriques, etc. Difficile à repérer et à traiter, la radicalisation est donc un enjeu majeur de sécurité nationale.

b) Comment identifier une situation de radicalisation ?

Pris isolément, un des comportements listés ci-dessous ne signifie pas qu'il y a radicalisation. C'est la combinaison de plusieurs comportements qui donne une forme de cohérence et qui doit provoquer l'étonnement.

Certaines combinaisons de comportements ou de traits de caractère sont des signaux forts de radicalisation et doivent attirer votre attention[16], que ce soit dans votre environnement quotidien ou sur votre lieu de travail.

COHÉRENCE → ÉTONNEMENT → SIGNALEMENT

Les signaux de rupture :

- changements physiques et vestimentaires ;
- propos asociaux ;
- passage soudain à une pratique religieuse hyper ritualisée ;
- rejet de l'autorité et de la vie en collectivité ;
- rejet brutal des habitudes quotidiennes ;
- repli sur soi ;
- haine de soi, rejet de sa propre personne, déplacement de la haine de soi sur autrui ;
- rejet de la société et de ses institutions (école, etc.) ;
- éloignement de la famille et des proches ;
- modification soudaine des centres d'intérêt.

15- Plaquette d'information contre la radicalisation, document du ministère de l'Intérieur (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, consulté le 12/07/2016.

16- *Guide interministériel de prévention de la radicalisation*, document du Comité interministériel de prévention de la délinquance, mars 2016, page 103.

Environnement personnel de l'individu :

- une image paternelle ou parentale défaillante, voire dégradée, ainsi qu'un environnement fragilisé ;
- les réseaux relationnels déjà inscrits dans une dépendance à une personne, à un groupe ou à des sites Internet ;
- immersion dans une famille radicalisée.

Théories et discours :

- théories conspirationnistes telles que des allusions à la fin du monde, complotistes et victimaires ;
- vénération des terroristes ;
- pratique de discours haineux et très violents envers une communauté ou une religion ;
- prosélytisme ;
- participation à des groupes religieux sectaires ou à des cercles de réflexion radicaux ;
- participation à des conférences de prédicateurs religieux extrémistes ;
- comportement binaire, distinguant le « pur » de l'« impur ».

Les techniques :

- usage des réseaux virtuels ou humains ;
- stratégies de dissimulation ou de duplicité ;
- planification de déplacements vers des zones de guerre.

c) Pourquoi lancer une démarche de signalement ?

Il s'agit de **prévenir, voire d'éviter, le basculement vers un comportement violent,** ainsi que d'accompagner les jeunes et les familles par des cellules adaptées au sein des préfectures de leur département de résidence.

L'objectif du signalement est de **protéger l'intéressé en l'empêchant de commettre un acte criminel** (pour le sortir au plus tôt du chemin sur lequel il s'est engagé peut-être malgré lui) et de **protéger la population** de possibles comportements violents[17].

Prendre l'initiative d'appeler le numéro vert constitue un simple signalement. Il appartiendra aux spécialistes d'en évaluer le caractère sérieux et la gravité.

d) Que se passe-t-il après un signalement ?

Si la situation est jugée préoccupante par les services de l'Etat, la personne faisant l'objet du signalement ainsi que sa famille **bénéficieront d'un accompagnement spécialisé et adapté à leur situation.**

Votre identité ne sera pas dévoilée, les signalements sont strictement confidentiels.

Même si vous n'êtes pas sûr d'avoir reconnu des combinaisons de signes de comportement suspect, **vous pourriez sauver des vies.** Il est donc préférable d'appeler rapidement le numéro vert. Des spécialistes se chargeront de qualifier la situation de préoccupante ou non.

Signaler une situation ne vous sera jamais reproché. Il n'est jamais trop tard pour signaler une situation de radicalisation.

Appeler le numéro vert :
0 800 005 696

Remplir le formulaire en ligne :
http://www.stop-djihadisme.gouv.fr/une-question-un-doute.html

17- *Guide interministériel de prévention de la radicalisation, op. cit.*, page 7.

2.2. Prévention de passage à l'acte violent et signalement de situations suspectes

Chaque citoyen a un rôle à jouer dans la prévention d'un passage à l'acte violent. En signalant un comportement dangereux, vous pouvez éviter qu'un acte criminel soit commis ou limiter sa portée, et ainsi sauver des vies. Tout citoyen a le droit d'être protégé mais il a le devoir d'agir.

2.2.1. Pourquoi signaler une situation suspecte ?

Dans un contexte de menace terroriste particulièrement élevée, il est plus que jamais nécessaire d'être attentif, au quotidien, au monde qui nous entoure.

L'organisation d'un attentat requiert le plus souvent une préparation et des moyens humains et matériels. **La plupart des attaques terroristes font d'abord l'objet d'un repérage** pour identifier les mesures de sécurité mises en place afin de les contourner, les chemins d'accès, etc. A l'occasion des différentes phases de l'élaboration d'une telle opération, **les terroristes sont contraints, à un moment ou à un autre, de s'exposer.**

En étant attentif à son environnement quotidien, **tout citoyen peut remarquer et signaler des faits, objets ou comportements pouvant indiquer un possible passage à l'acte.** L'expérience a montré que de simples indices repérés par un passant ou par un voisin pouvaient permettre de prévenir une attaque terroriste.

L'attention de tout un chacun, portée à des détails simples, sauve des vies.

2.2.2. Comment détecter une situation suspecte ?

Certains comportements ou certaines situations peuvent sembler incohérents dans un environnement donné. Vous devez savoir vous étonner de ces incohérences et vous demander si cela ne mérite pas un signalement.

La préparation d'une action terroriste n'a pas toujours la perfection que l'on imagine ou que l'on voit dans les séries télévisées. Des incohérences apparaissent et vous pouvez les détecter. **Faites appel à votre bon sens et à votre intuition.**

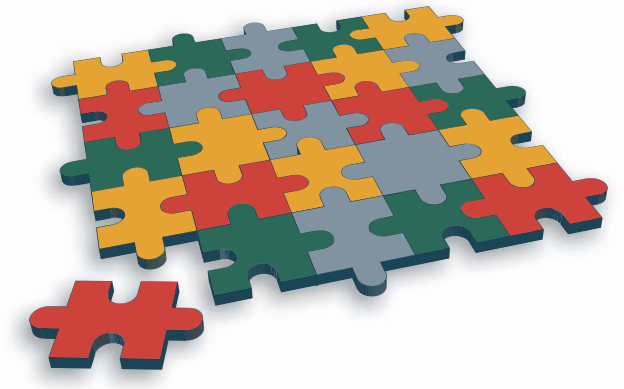
Détecter un comportement suspect, c'est donc savoir s'étonner de l'incohérence entre un détail et une situation ou de l'inadéquation de l'attitude d'une personne avec un lieu. **Toute incohérence vous laissant penser qu'une action violente est en cours de préparation doit vous interpeller, vous étonner et cela doit vous conduire à effectuer un signalement.**

Il faut par conséquent apprendre à être un observateur de son environnement (voisinage, vie professionnelle, transports en commun, etc.).

INCOHÉRENCE → ÉTONNEMENT → SIGNALEMENT

Comment une action terroriste est-elle planifiée ?

Comprendre la manière dont se planifie une action violente peut vous aider à déceler certains indices de préparation. Quel que soit le niveau d'expérience des terroristes, ils prépareront leur action de la manière suivante : choix des cibles, préparation de l'action et mise en place.



La préparation d'un acte terroriste laisse un ensemble d'indices qui, telles les pièces d'un puzzle, peuvent être assemblés par les forces de sécurité pour déjouer un projet d'attentat.

a) Le choix des cibles

Les actions terroristes peuvent viser des cibles symboliques (des personnalités, une communauté, un corps de métiers représentant l'Etat, etc.) ou indiscriminées (population dans son ensemble) pour créer un climat de terreur et toucher les intérêts économiques du pays.

b) La préparation de l'action

Les terroristes conduisent nécessairement des reconnaissances de la cible visée pour en identifier les vulnérabilités et déterminer le mode d'action qui leur permettra d'atteindre l'objectif visé :

- **reconnaissance physique du site ciblé,** seul, en binôme ou en groupe (possible communication par gestes, chronométrage, présence d'une même personne sur le même lieu plusieurs fois sans raison apparente, stationnement prolongé d'un véhicule avec des personnes à bord, etc.) ;
- **rassemblement d'un maximum d'informations** sur la cible :
  - recherches de complicités internes ;
  - demandes de renseignements sur les mesures de sécurité par le biais de discussions en apparence anodines ;
  - observation de la manière dont se déroulent les contrôles de sécurité, voire test de ces mêmes contrôles via de fausses alertes (type alerte à la bombe) ;
  - prises de vues (photographie ou film) des infrastructures du site ciblé et du dispositif de protection mis en place (porte d'entrée d'un ministère, patrouille de militaires, etc.) ;
  - prises de notes sur les dispositifs de sécurité (plan du site, positionnement des caméras de surveillance, des portes d'entrée et de sortie, etc.) ;
  - recherches d'informations par Internet (réseaux sociaux, plans et vues aériennes, etc.).
- utilisation de **techniques de dissimulation ou de camouflage** (qui peuvent être identifiées par l'entourage de proximité) : utilisation de pseudonymes ou de plusieurs pièces d'identité avec des noms différents, recours à des cartes téléphoniques prépayées ou à plusieurs téléphones portables, etc.

c) La phase précédant l'action

Un individu sur le point de commettre une attaque terroriste dissimulera probablement des armes : couteau, fusil d'assaut, arme de poing, ceinture d'explosifs, munitions, etc. Il aura donc une tenue adaptée et pourra :

- porter un sac anormalement lourd ou déformé par une arme ;
- porter des protections (genouillères, gilet pare-balles) ;
- avoir une tenue inappropriée pour la saison ou suffisamment ample pour cacher une arme ;
- dissimuler une arme dans le dos afin de franchir un point de contrôle qui se limiterait à l'ouverture des vestes sans palpation ;
- montrer des signes de nervosité ou de méfiance en contraste avec l'environnement.

Une attaque à l'explosif peut également être réalisée. Certaines situations doivent vous alerter :

- une lettre ou un colis avec une adresse mal renseignée, portant des traces ou dégageant des odeurs peuvent contenir de l'explosif ;
- un colis ou un sac abandonné. Un sac posé dans un lieu de passage important doit entraîner un signalement ;
- un véhicule en stationnement prolongé depuis longtemps à proximité d'un lieu de rassemblement (marché, lieu de culte, etc.) ou d'un site sensible (mairie, ambassade, etc.). Un véhicule piégé ne sera pas mis en place au hasard, il sera situé à proximité de la cible visée. Un véhicule sans plaque d'immatriculation doit vous interpeller.

2.2.3. Comment signaler et réagir ?

a) Pour tous les citoyens

Si vous êtes témoin d'un comportement suspect, restez discret. Ne montrez pas à la personne repérée que son attitude vous surprend. **Observez et mémorisez des éléments objectifs** qui pourraient être transmis à la police ou à la gendarmerie nationale (plaque d'immatriculation, modèle de véhicule, description précise des individus, direction de fuite, etc.). Pour que votre signalement puisse être utile aux forces de sécurité intérieure, les éléments objectifs que vous pourrez donner sont absolument essentiels.

OBSERVER → MÉMORISER → SIGNALER

Appelez les forces de sécurité intérieure au **17, 112 ou 114** (pour les personnes ayant des difficultés à entendre ou à parler).

En cas d'urgence dans un train :

- **Appelez le 31 17 ou envoyez un SMS au 31 177**. Si vous appelez en utilisant l'**application Alerte 3117**, votre interlocuteur vous géolocalisera. Décrivez le lieu de l'attaque : le numéro du train ou sa situation géographique, le numéro de la voiture, etc.

b) Pour les employés d'un site sensible ou accueillant du public

Des procédures internes doivent permettre la remontée très rapide d'un signalement.

Si un employé observe des actions ou des comportements suspects, celui-ci :

- peut engager une conversation normale avec l'individu dont le comportement a été remarqué ;
- doit informer ses supérieurs.

En posant des questions ouvertes[18], l'employé pourra peut-être déterminer si l'individu repéré par son comportement dissimule de mauvaises intentions. Dans le cas où un individu préparerait une action malveillante, celui-ci pourrait adopter un comportement fuyant, nerveux ou agressif.

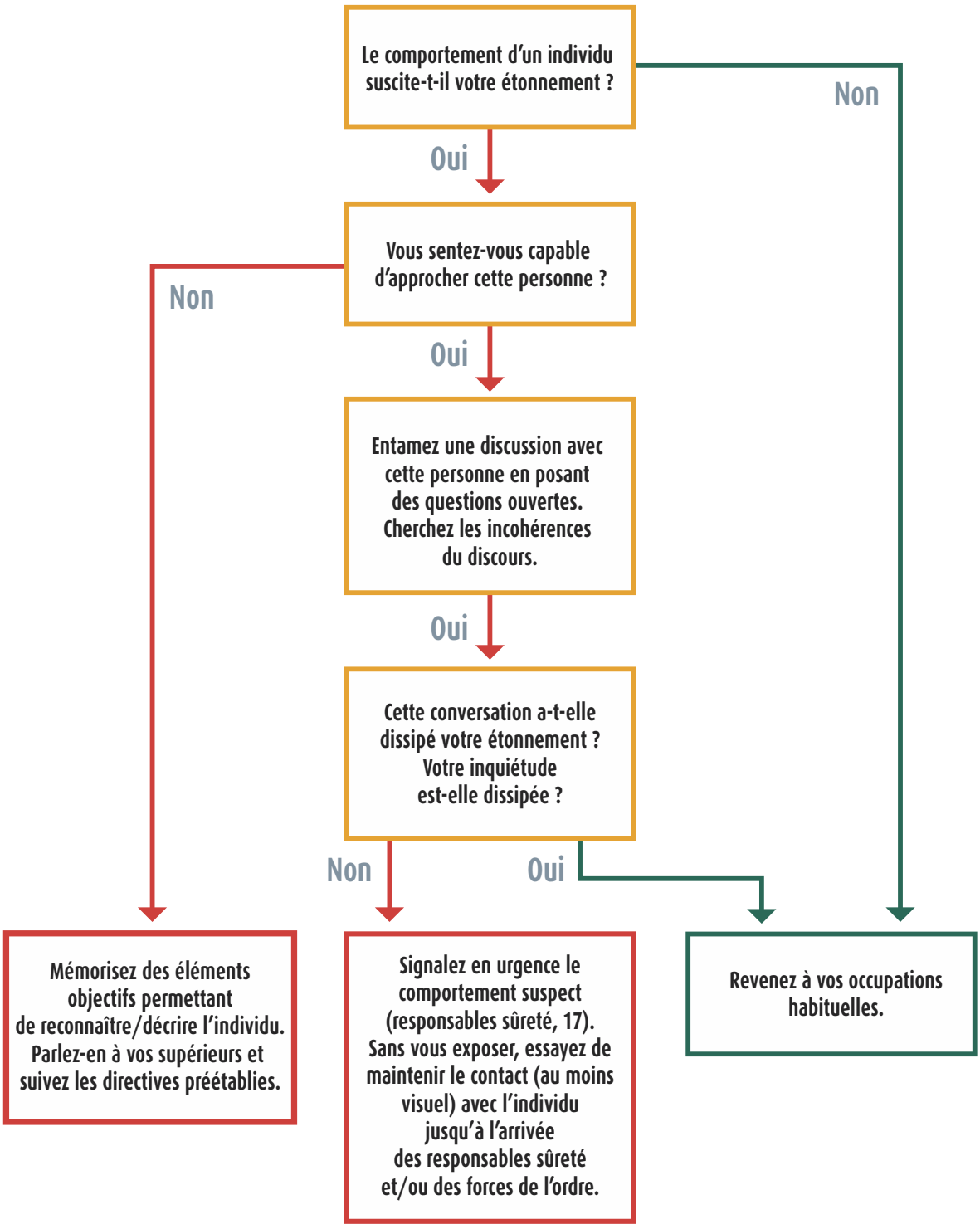
Par exemple, si un individu inconnu est repéré à l'intérieur d'une zone non ouverte au public, l'employé pourrait demander qui cette personne souhaite rencontrer. De même, si un individu prend des photos laissant penser à une reconnaissance, l'employé peut demander ce qui suscite l'intérêt de l'individu.

Les employés, et notamment ceux en charge de la sécurité des biens et des personnes, doivent être sensibilisés dans la mesure du possible à ce type de situations et à la réaction à adopter.

Les opérateurs peuvent sensibiliser leurs employés par des mises en scène concrètes leur permettant d'acquérir les bonnes réactions et attitudes.

18- Questions auxquelles on ne peut pas répondre par « oui » ou par « non ».

Exemple d'aide à la décision d'un employé de site sensible ou accueillant du public face à un comportement suspect.



2.2.4. Que faire en cas de survol de drones ?

Considérés comme des jouets, les drones constituent pourtant une menace qui doit être prise très au sérieux. En effet, des personnes malveillantes peuvent s'en servir pour collecter des informations en vue de la préparation d'un acte terroriste. De plus, il ne faut pas oublier qu'un drone peut également représenter une arme du fait de sa capacité d'emport (grenade, arme chimique ou biologique, etc.), voire une arme par destination.

a) Qu'est-ce qu'un drone malveillant ?

Les aéronefs civils circulant sans personne à bord, communément appelés drones, sont régis par deux arrêtés du 17 décembre 2015[19]. En vertu de ces derniers, et sauf dérogations, il est notamment interdit de faire voler un drone au-dessus de l'espace public en agglomération, de même que la nuit.

Ainsi, un drone survolant un rassemblement de personnes ou évoluant de nuit doit être considéré comme potentiellement malveillant. Potentiellement en effet, car il peut également s'agir d'un acte non intentionnel de négligence ou de maladresse de la part d'un télépilote « loisir »[20].

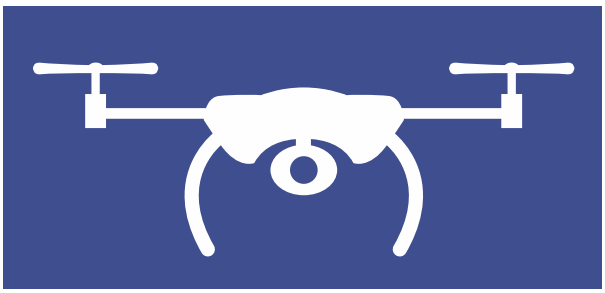
b) Qui prévenir ?

En cas de situation anormale, alertez les forces de sécurité (17).

Attention toutefois à ne pas saturer les autorités, les informations doivent être pertinentes, notamment dans les cas de survol de nuit.

c) Que faut-il décrire ? (liste non exhaustive)

- Où ? Quand ? Quoi ? Combien ?
- L'altitude de vol, sa provenance et sa direction.
- Le type de drone (multirotor ou aile volante, propulsion électrique ou moteur thermique, type de lumières).
- Transporte-t-il une charge externe (caméra ou autre) ?
- Si le télépilote a pu être repéré, faire une description physique et comportementale.



19- Sur ces 2 arrêtés, voir rubrique « *En savoir plus* » page 70.

20- Souvent le télépilote se trouve à vue de son drone, c'est-à-dire dans un rayon inférieur à 500 m de l'engin. Selon son comportement, la nature du survol pourra être déterminée.

3. RÉAGIR

3.1. Que faire en cas d'attaque armée ?

Une attaque armée est exécutée par un ou plusieurs individus dont l'intention est soit de faire un maximum de victimes sans distinction, soit de cibler spécifiquement certaines personnes ou lieux symboliques.

Les agresseurs peuvent utiliser principalement des armes à feu, des armes blanches (couteau, hache) ou des ceintures explosives.

Les recommandations que vous allez lire ci-dessous seront d'autant plus faciles à exécuter que des exercices auront été réalisés avant.

3.1.1. Cas général

Déterminez la réponse la plus appropriée à la situation. Celle-ci n'est pas figée, elle évolue : adoptez vos modes de réaction aux circonstances.

***Si l'attaque est extérieure au site* dans lequel vous vous trouvez,** il est recommandé de rester à l'abri.

***Si l'attaque a lieu à l'intérieur du site* où vous vous trouvez,** respectez les consignes de sécurité présentées ci-dessous.

a) S'échapper

Condition 1 : être certain que vous avez identifié la localisation exacte du danger.

Condition 2 : être certain de pouvoir vous échapper sans risque.

Dans tous les cas :

- ne déclenchez pas l'alarme incendie ;
- laissez toutes vos affaires sur place ;
- ne vous exposez pas (courbez-vous, penchez-vous) ;
- prenez la sortie la moins exposée et la plus proche ;
- utilisez un itinéraire connu ;
- aidez si possible les autres personnes à s'échapper ;
- prévenez / alertez les autres personnes autour de vous ;
- dissuadez toute personne de pénétrer dans la zone de danger.

RÉAGIR EN CAS D'ATTAQUE TERRORISTE

AVANT L'ARRIVÉE DES FORCES DE L'ORDRE, CES COMPORTEMENTS PEUVENT VOUS SAUVER

1/ S'ÉCHAPPER *si c'est impossible* 2/ SE CACHER

3/ ALERTER ET OBÉIR AUX FORCES DE L'ORDRE

VIGILANCE

- Témoin d'une situation ou d'un **comportement suspect**, vous devez contacter les forces de l'ordre (17 ou 112)
- Quand vous entrez dans un lieu, repérez les **sorties de secours**

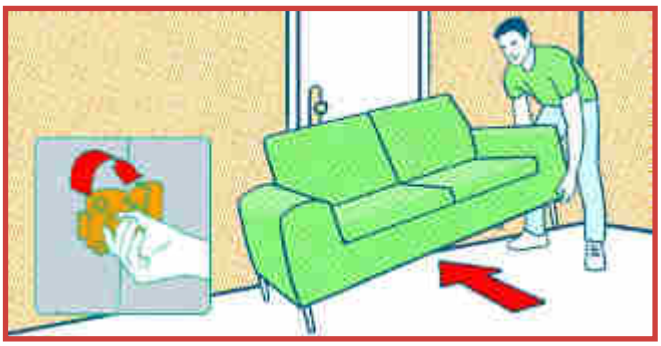
- Ne diffusez aucune information sur l'intervention des forces de l'ordre
- Ne diffusez pas de rumeurs ou d'**informations non vérifiées** sur internet et les réseaux sociaux
- Sur les réseaux sociaux, **suivez les comptes @Place_Beauvau et @gouvernementfr**

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Pour en savoir plus :
www.gouvernement.fr/reagir-attaque-terroriste

VIGIPIRATE

b) S'enfermer



- dans la mesure où vous ne pouvez pas vous échapper, **enfermez-vous, barricadez-vous,** cachez-vous dans un endroit hors de la portée des agresseurs ;
- **condamnez la porte** si celle-ci n'a pas de serrure en bloquant la poignée avec des moyens de fortune (meuble, etc.) ;
- **éteignez les lumières ;**

- éloignez-vous des murs, portes et fenêtres ;
- **allongez-vous au sol** derrière plusieurs obstacles solides (des projectiles tirés au travers des cloisons peuvent atteindre l'intérieur de la pièce dans laquelle vous vous trouvez) ;
- **faites respecter le silence** absolu (portables en mode silence, sans vibreur) et décrochez les téléphones fixes ;
- restez proche des personnes manifestant un stress et rassurez-les ;
- attendez l'intervention des forces de sécurité.

c) Alerter

Une fois en sécurité :

- prévenez les forces de sécurité [17, 112 ou 114 (personnes ayant des difficultés à entendre et à parler)], en essayant de donner les informations essentielles :
  - **Où ?** Donnez votre position mais également celle de vos agresseurs ;
  - **Quoi ?** Nature de l'attaque (explosion, fusillade, prise d'otages…), type d'armes (arme à feu, arme blanche, explosifs…), estimation du nombre de victimes ;
  - **Qui ?** Estimation du nombre d'assaillants, description (sexe, vêtements, physionomie, signes distinctifs…), attitude (comment se comportent-ils, regardent-ils la télévision, ont-ils des moyens de communication…). Estimation du nombre de personnes blessées ou cachées autour de vous.

- Si vous ne pouvez pas parler, appelez et laissez la ligne en suspens pour que les forces de sécurité puissent être prévenues.

NE PENSEZ PAS QUE D'AUTRES ONT DONNÉ L'ALERTE, FAITES-LE !

d) Résister

Si se cacher ou évacuer est impossible et si votre vie est directement en danger et dans la mesure de vos moyens, **résistez en dernier recours.**

Collectivement, la prise d'ascendant sur un adversaire isolé peut retourner la situation.

Des gestes simples peuvent contribuer à interrompre ou neutraliser la menace comme suit :

- distrayez l'adversaire (criez) et attaquez ;
- profitez d'un moment de vulnérabilité de l'agresseur (changement de chargeur, etc.) ;
- jetez des objets / utilisez des armes improvisées.

Attention, le cas d'une prise d'otages est différent d'une fusillade de masse. Ne cherchez pas la confrontation avec les terroristes et respectez leurs consignes.

e) Faciliter l'intervention des forces de sécurité et des services de secours

Afin de faciliter l'intervention des forces de sécurité et des services de secours :

- restez enfermé jusqu'à ce que les forces de sécurité procèdent à l'évacuation ;
- **évacuez calmement, les mains ouvertes** et apparentes pour éviter d'être perçu comme un suspect ;
- **ne courez pas en direction des forces de l'ordre** ;
- **signalez les blessés** et l'endroit où ils se trouvent, portez les gestes de premiers secours si vous en avez reçu la formation ;
- ne quittez pas les lieux immédiatement : votre témoignage pourrait faire avancer l'enquête.

3.1.2. Cas particuliers

a) En cas d'attaque à l'arme blanche

- **enfuyez-vous** ;
- **si vous ne pouvez pas vous enfuir :** protégez-vous avec un bouclier de fortune (sac, chaise, vêtement enroulé sur l'avant-bras, etc.) ;
- **utilisez une arme de fortune** permettant de prolonger votre bras ;
- **attaquez à plusieurs :** une personne peut attirer l'attention de l'agresseur tandis qu'une autre cherche à le neutraliser.

Un agresseur muni d'une arme blanche peut être déstabilisé par une réaction collective des victimes ou des personnes situées à proximité. Dans la mesure du possible, se concerter avant d'agir et attaquer par surprise.

b) En cas d'explosion ou de risque explosif

- **éloignez-vous du lieu de l'explosion** ;
- **ne touchez à rien** (objet, sac abandonné, débris) ;
- **protégez-vous / mettez-vous à l'abri** derrière un obstacle solide (une deuxième explosion, à proximité du premier lieu d'explosion, visant les secours ou les forces de l'ordre, est possible) ;
- attendez l'intervention des secours.

c) En cas d'attaque dans un train

Se cacher

Allongez-vous sous les sièges ou accroupissez-vous.

Alerter

Appelez le 31 17 ou envoyez un SMS au 31 177. Si vous appelez en utilisant l'application Alerte 3117, votre interlocuteur vous géolocalisera. Décrivez le lieu de l'attaque : le numéro du train ou sa situation géographique, le numéro de la voiture, etc.

Résister

En dernier ressort, si votre vie est menacée, gênez ou neutralisez l'action des terroristes avec l'aide des personnes cachées autour de vous.

S'échapper

Ne sortez du train que si vous pouvez le faire sans traverser de voie ferrée.

Faciliter l'intervention des forces de sécurité et des services de secours

A l'arrivée des forces de l'ordre, mettez vos mains en évidence et restez immobile.

d) En cas d'attaque dans un métro

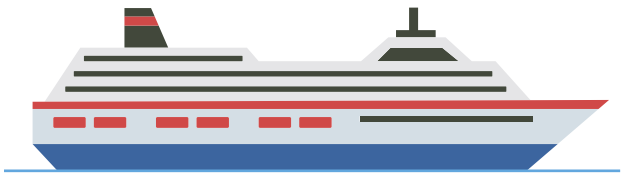
Appelez le 31 17 ou envoyez un SMS au 31 177.

Utilisez les bornes d'appel des quais de station ou prenez contact avec des agents.

e) En cas d'attaque sur un navire en mer

S'éloigner de la menace

- si la taille et l'architecture du navire le permettent, éloignez-vous du lieu de l'agression et laissez vos affaires sur place ;
- **ne vous jetez pas à l'eau.**



Suivre les consignes de bord

Se cacher

- si vous êtes loin de votre cabine : cachez-vous, confinez-vous et évitez les attroupements ;
- si vous êtes à proximité de votre cabine : enfermez-vous dans votre cabine ;
- si vous êtes parvenu à vous confiner dans une pièce : bloquez l'entrée, fermez les portes, dissimulez-vous et n'ouvrez sous aucun prétexte ;
- masquez votre présence : éteignez toutes les sources sonores et lumineuses.
  ATTENTION : ne pas éteindre votre téléphone, le mettre en mode silencieux.

3.2. Que faire en cas de cyberattaque ?

Pendant une attaque

En cas de cyberattaque, **signalez les faits rapidement** aux services spécialisés via la plateforme de signalement **PHAROS**[21] ou par téléphone au numéro dédié.

Après une attaque

Si vous avez été victime d'une attaque de nature cyber, **déposez plainte** auprès d'un service de police nationale ou de gendarmerie nationale ou bien adressez un courrier au procureur de la République auprès du tribunal de grande instance compétent, en plus du signalement.

Munissez-vous d'un maximum de renseignements sur l'attaque constatée. Des services spécialisés se chargent ensuite de l'enquête. N'hésitez pas à consulter le site « risques.gouv.fr » pour connaître les différents comportements à adopter en fonction du type d'attaque dont vous avez pu être victime.

Enfin, soyez attentif aux consignes et recommandations transmises par les autorités concernant les bonnes pratiques à adopter sur Internet.

La cybervigilance

En situation de crise, la circulation de l'information est un élément essentiel pour la bonne gestion des événements. Etre cybervigilant, c'est aussi s'assurer de ne pas diffuser des informations erronées pouvant altérer la gestion de la crise. **Pendant une attaque, ne relayez en aucun cas les rumeurs.**

- Restez attentif aux consignes émanant de sources officielles :
  - Agence nationale de la sécurité des systèmes d'information (ANSSI) : recommandations techniques suite à un événement cyber ;
  - Service d'information du Gouvernement, ministère de l'Intérieur (gendarmerie, police, préfecture) et collectivités locales ;
  - Autres ministères concernés par la crise.

21- Site de signalement: https://www.internet-signalement.gouv.fr/

3.3. Que faire en cas d'attaque avec un produit toxique ?

De nombreux produits toxiques sont utilisés dans l'industrie (le chlore, par exemple). Certains d'entre eux ont déjà été détournés par des groupes terroristes à des fins de guerre. Ces produits sont susceptibles d'être volontairement libérés sur des sites à forte affluence.

La pénétration des produits toxiques dans l'organisme peut se faire selon différentes modalités. **Ils peuvent, par inhalation, par contact avec la peau ou les yeux ou par ingestion, provoquer de graves lésions :** brûlures, œdème du poumon, asthme, etc. Ces lésions peuvent être limitées, voire empêchées, si l'on adopte les bons comportements détaillés dans l'infographie en page suivante :

- **restez calme et rejoignez aussi rapidement que possible une zone plus sûre** tout en aidant les personnes les plus vulnérables (images de 1 à 4) ;
- **limitez l'intoxication en vous déshabillant** et en vous lavant afin de réduire ou d'éliminer le produit toxique pour qu'il ne constitue plus un risque. Empêchez-le de se propager à d'autres personnes (image 5) ;
- **contactez au plus vite les services de secours et de soins en appelant le : 15, 18, 112 ou 114** (image 6) ;
- **restez sur place pour ne pas contaminer les autres personnes,** y compris les personnels de secours et de soins, et attendez les secours afin qu'ils vous dispensent les premiers soins (images 7 et 8) ;
- **dans tous les cas : ne buvez pas, ne vous frottez pas le visage, ne mangez pas, ne fumez pas et évitez le contact avec d'autres personnes** (image 9).

QUE FAIRE EN CAS D'EXPOSITION À UN GAZ TOXIQUE

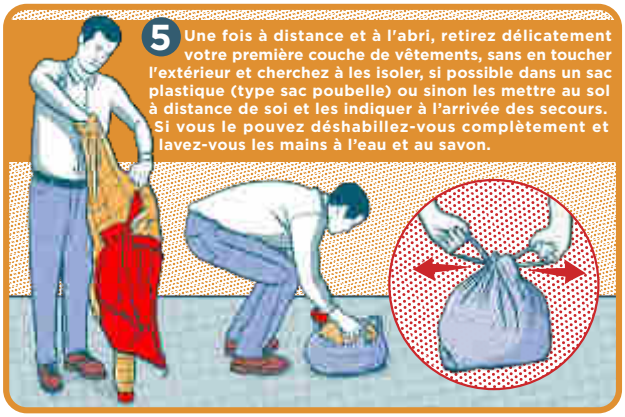
AVANT L'ARRIVÉE DES SECOURS, CES COMPORTEMENTS PEUVENT VOUS SAUVER LA VIE...

1 Protégez votre nez et votre bouche par tous les moyens possibles : mouchoir, foulard ou tissu humides

2 Même si vous vous sentez mal, ne vous allongez pas, ne vous asseyez pas, vous pourriez ne plus vous relever.

3 Quittez rapidement les lieux semblant présenter un danger (si odeur anormale, si des personnes larmoient ou font des malaises...)

4 Si vous apercevez des gens en train de s'évanouir ou de suffoquer, aidez-les à sortir de la zone sans revenir sur vos pas.



5 Une fois à distance et à l'abri, retirez délicatement votre première couche de vêtements, sans en toucher l'extérieur et cherchez à les isoler, si possible dans un sac plastique (type sac poubelle) ou sinon les mettre au sol à distance de soi et les indiquer à l'arrivée des secours. Si vous le pouvez déshabillez-vous complètement et lavez-vous les mains à l'eau et au savon.

6 Utilisez votre portable uniquement pour alerter les secours en précisant votre emplacement et s'il faut intervenir rapidement sur un cas grave.

Pompiers : 18 ou 112
SAMU : 15

7 Ne rentrez surtout pas chez vous. Ne vous rendez pas de vous-même à l'hôpital. Attendez impérativement les secours et suivez leurs consignes, vous risqueriez de contaminer vos proches !

8 Les services de secours organisent un point de rassemblement où des soins vous seront donnés.

9 Ne serrez pas les mains, ne buvez pas, évitez de vous frotter le visage, ne mangez pas, ne fumez pas.

RESTEZ CALME, VOUS FACILITEREZ L'ORGANISATION DES SECOURS ET DES SOINS.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

ATTENTION !

Certains symptômes graves peuvent survenir plusieurs heures après l'intoxication.

Dans ce cas, appelez sans tarder le 15, rappelez que vous étiez dans la zone toxique et suivez les consignes que l'on vous donnera.

Sur les réseaux sociaux, suivez les comptes @Place_Beauvau et @gouvernementfr
Restez à l'écoute des consignes des autorités publiques.

VIGIPIRATE

4. GÉRER L'APRÈS-ATTENTAT

4.1. Vous avez été témoin d'une attaque terroriste

Contactez les services de police et de gendarmerie pour signaler ce que vous avez vu sur les lieux de l'attentat et donnez tous les détails qui pourraient faire avancer l'enquête. Réservez aux seules autorités les photos ou les vidéos que vous auriez pu prendre lors d'une attaque.

4.2. Vous avez été victime d'une attaque terroriste

À la suite d'un acte terroriste, les victimes sont prises en charge par les services d'urgence. Elles bénéficient ensuite d'un dispositif renforcé d'aide aux victimes et d'une indemnisation. Ce dispositif est piloté par le secrétariat d'Etat chargé de l'Aide aux victimes.

4.2.1. La prise en charge en urgence

Sur les lieux de l'acte terroriste ou à proximité, vous pouvez vous signaler aux forces de police et de gendarmerie ou aux services de secours. Des cellules d'urgence médico-psychologique sont chargées de vous prendre en charge et d'assurer une première intervention destinée notamment à réduire les risques de choc post-traumatique.

En cas d'attaque terroriste d'ampleur, la Cellule interministérielle d'aide aux victimes (CIAV) peut être activée par le Premier ministre. Elle est chargée d'informer les victimes et leurs familles sur le dispositif mis en place et sur leurs droits. Un centre d'accueil des familles et différents lieux de prise en charge médico-psychologique pourront être mis en place.

4.2.2. L'aide aux victimes de terrorisme

Pour répondre aux attentes et aux besoins des victimes, un secrétariat d'Etat chargé de l'Aide aux victimes, placé sous l'autorité du Premier ministre, a été créé en France en mars 2016. Il est chargé de protéger et d'assurer les droits des victimes. En cas de terrorisme, les victimes bénéficient de dispositifs spécifiques et protecteurs.

Pour obtenir des renseignements, se faire expliquer les démarches à entreprendre en fonction de la situation (perte d'un proche, blessé physique/psychologique, proche d'un blessé…), être orienté (prise en charge psychologique, dépôt de plainte, organisation des obsèques, indemnisation des préjudices, organisation de la succession, etc.), constituer un dossier, vous pouvez :

consulter le site Internet créé pour simplifier les démarches des victimes d'actes de terrorisme :

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

Ce site permet aux victimes :

- de connaître et d'effectuer les démarches en ligne ;
- de déposer et de suivre une demande auprès du Fonds de garantie des victimes des actes de terrorisme et d'autres infractions (FGTI) et auprès de l'Office national des anciens combattants et des victimes de guerre (ONAC-VG) ;
- de trouver les coordonnées d'associations d'aide aux victimes.

Appeler le 08 842 846 37 (7 jours sur 7)

Point d'entrée unique pour toutes les victimes, cette plateforme pourra vous orienter vers l'une des 132 associations d'aide aux victimes conventionnées par le ministère de la Justice sur l'ensemble du territoire. Les professionnels de ces associations, juristes, psychologues et travailleurs sociaux, sont chargés de vous accueillir gratuitement pour :

- vous écouter et vous informer sur l'ensemble des droits qui vous sont reconnus, sur le fonctionnement judiciaire et sur les dispositifs d'indemnisation pour les victimes d'actes de terrorisme ;
- faciliter vos démarches auprès des organismes comme le FGTI, l'ONAC-VG, la CPAM (Caisse primaire d'assurance maladie), la CAF (Caisse d'allocations familiales), l'administration fiscale ;
- vous proposer un soutien psychologique en relais des prises en charge en urgence dont vous avez peut-être déjà bénéficié ;
- vous orienter vers des professionnels (avocat, médecin-conseil…).

Contacter le SAMU (15)

Les victimes d'acte terroriste peuvent bénéficier d'un soutien médico-psychologique partout en France. En composant le 15 (24 heures sur 24), le SAMU réorientera votre appel vers une cellule d'urgence médico-psychologique (CUMP). La CUMP pourra vous prendre en charge et, si besoin, vous proposer un suivi dans la durée dans les structures publiques de votre département.

4.2.3. Une indemnisation pour les victimes d'actes de terrorisme : le FGTI

Les victimes d'actes de terrorisme peuvent, sous certaines conditions, être indemnisées par le Fonds de garantie des victimes des actes de terrorisme et d'autres infractions (FGTI).

Pour plus d'informations, rendez-vous sur le site :

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

4.2.4 Déposer plainte

Vous pouvez déposer plainte en France auprès de l'antenne de police judiciaire la plus proche de votre domicile. Pour connaître la localisation de cette dernière, vous pouvez téléphoner au commissariat de police ou à la brigade de gendarmerie la plus proche de votre domicile, afin que vous soient communiquées les coordonnées de l'antenne de police judiciaire la plus proche.

PARTIE 3

LES DOMAINES D'ACTION

Cette partie vise à détailler les spécificités de chacun des domaines d'action du plan VIGIPIRATE.

1. ALERTER ET MOBILISER

Description du domaine

L'alerte vise à **transmettre une information dans l'urgence à tous les acteurs concernés afin de mobiliser immédiatement les moyens d'intervention et d'adapter les mesures de protection.** Il s'agit aussi de faire adhérer la population par une communication permettant d'entretenir la vigilance permanente et de susciter une mobilisation citoyenne en cas d'événement grave.

Certains secteurs d'activité ont leurs propres chaînes. Ces chaînes d'alerte mettent en relation les ministères concernés, les administrations et services déconcentrés de l'Etat et les opérateurs. Les opérateurs d'importance vitale ont, quant à eux, des obligations légales particulières en matière d'alerte et d'intervention.

Stratégie de sécurité

La stratégie de sécurité répond à une double logique d'information et de réactivité. Elle vise à **alerter** et à **communiquer le plus largement possible, tout en mobilisant des moyens nationaux spécialisés (tels que les capacités de lutte contre la menace de diffusion de produits toxiques).**

A titre d'exemple, dans le cadre de la préparation de l'Eurofoot 2016, des moyens spécialisés importants de la sécurité civile, des forces de sécurité intérieure, du SAMU et des armées ont ainsi été mis en alerte ou déployés.

2. PROTÉGER LES RASSEMBLEMENTS DE MASSE

Description du domaine

Un rassemblement se caractérise par le regroupement public d'un nombre important de personnes dans un lieu ouvert. La protection des rassemblements concerne plusieurs types d'acteurs : **les organisateurs, l'autorité administrative** (maires, préfets), **les forces de l'ordre** (police, gendarmerie, polices municipales).

Les organisateurs sont responsables de la sécurité générale du rassemblement, particulièrement celle des participants. Un service de sécurité propre doit veiller au bon déroulement du rassemblement (filtrage des accès, contrôle des personnes, service d'ordre) et assurer la liaison avec les forces de l'ordre. Il peut être confié au secteur privé.

L'autorité administrative est responsable de l'ordre public. Elle vérifie les mesures prévues par les organisateurs au regard de la nature du rassemblement, de l'importance du public attendu, de la configuration des lieux et des circonstances propres à l'événement. En cas de risque de trouble à l'ordre public ou de menace particulière contre un rassemblement, elle peut l'interdire par un arrêté qu'elle notifie immédiatement aux organisateurs.

Les forces de l'ordre peuvent être engagées sur décision de l'autorité administrative en fonction de la nature ou de la vulnérabilité d'un rassemblement, pour des missions de régulation de circulation, de gestion de foule et de surveillance générale.

Stratégie de sécurité

La stratégie consiste à mettre en place des **dispositifs de surveillance et de contrôle qui s'appuient sur le principe de défense en profondeur.** En dernier recours, il peut être décidé, en fonction de la menace, de limiter, voire d'interdire le rassemblement.

Pour déterminer le niveau de protection d'un rassemblement, il est essentiel d'évaluer la menace à laquelle il est exposé. Une attention particulière doit ainsi être accordée aux rassemblements cumulant forte affluence, renommée touristique et symbole culturel, religieux ou politique. Les notes de posture VIGIPIRATE ont notamment pour objectif d'identifier les catégories de rassemblements les plus sensibles pour une période donnée.

3. PROTÉGER LES INSTALLATIONS ET BÂTIMENTS

Description du domaine

Le domaine des installations et bâtiments concerne **l'ensemble des édifices qui peuvent constituer des cibles potentielles, soit en raison de leur valeur symbolique, économique, politique ou écologique, soit en raison du public qu'ils accueillent.** Certaines infrastructures propres à des secteurs d'activités précis font l'objet de protections spécifiques, décrites dans les chapitres du plan VIGIPIRATE classifié qui leur sont consacrés. C'est le cas pour les transports, les installations dangereuses, les réseaux, la chaîne alimentaire et la santé.

Les pouvoirs publics sont chargés de la protection externe, qu'ils assurent notamment par la surveillance de la voie publique et la régulation de la circulation et du stationnement. Le dispositif est adapté en fonction du type d'installation, de sa configuration et de l'évaluation de la menace. Il peut employer des forces de l'ordre de nature différente : les services locaux, les polices municipales, la police nationale, la gendarmerie nationale, voire les armées.

Les responsables d'installations et bâtiments sont chargés de la protection interne et des accès aux bâtiments.

Stratégie de sécurité

La stratégie vise à **adapter la sécurité externe, en agissant sur la surveillance et sur les conditions de stationnement et de circulation aux abords des installations, la sécurité des accès et la sécurité interne, en agissant sur la surveillance et le contrôle des flux.** Elle s'appuie sur les principes de défense en profondeur et de responsabilité partagée entre les exploitants d'installations et les pouvoirs publics. Les notes de posture VIGIPIRATE précisent notamment les catégories de bâtiments devant faire l'objet d'une vigilance ou d'une protection particulière.

Enfin, aux mesures traditionnelles de sécurité des bâtiments, il faut ajouter les procédures, connues de tous, pour permettre la meilleure réaction possible de l'ensemble des personnels en cas d'intrusion malveillante, voire d'attaque terroriste. **La qualité de la préparation d'un établissement conditionne la qualité de sa réaction en cas de crise.**

4. PROTÉGER LES INSTALLATIONS ET MATIÈRES DANGEREUSES

Description du domaine

Le plan VIGIPIRATE s'intéresse aux activités industrielles ainsi qu'aux activités de stockage et de transport de certaines matières, en raison des risques qu'elles engendrent de par leur dangerosité.

Les pouvoirs publics définissent la réglementation applicable dans ce domaine, contrôlent son application et délivrent les autorisations d'exploitation. Dans le cas particulier du secteur nucléaire civil, le contrôle est assuré par l'Autorité de sûreté nucléaire (ASN), qui est une autorité indépendante.

Le plan VIGIPIRATE associe les entreprises du domaine qui ont des obligations de sécurité : celles classées SEVESO « seuil bas » ou « seuil haut », celles dont les activités sont soumises à autorisation et celles transportant des matières dangereuses. Il s'agit en particulier d'entreprises des secteurs de la chimie, des hydrocarbures et du nucléaire.

Le grand public est également concerné par la réglementation sur la commercialisation et l'utilisation des produits permettant de fabriquer des explosifs.

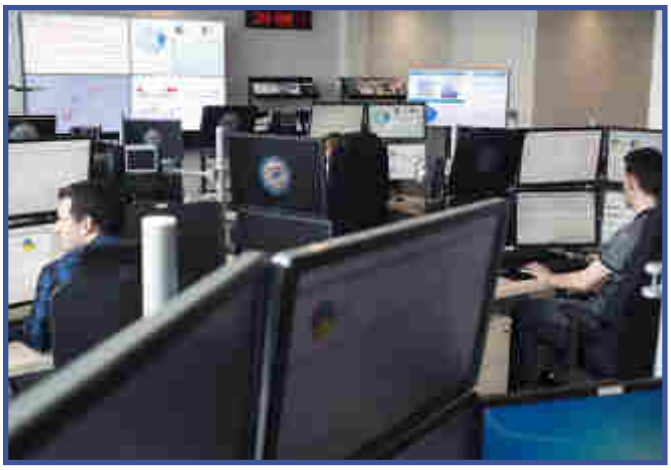
Stratégie de sécurité

La stratégie vise à **protéger les installations dangereuses,** les lieux de stockage des matières dangereuses ou sensibles, ainsi que les transports de ces matières.

La protection de ces installations consiste de surcroît à s'assurer qu'aucun acte malveillant ne puisse avoir de conséquences majeures sur les populations et l'environnement.

5. ASSURER LA CYBERSÉCURITÉ

Description du domaine



A l'heure du numérique et de la dématérialisation, **les systèmes d'information sont devenus une cible de choix pour les terroristes.** Aussi, les atteintes à leur bon fonctionnement par le biais d'attaques informatiques peuvent avoir de lourdes conséquences sur le plan national en portant atteinte à la vie ou à la santé des citoyens, en perturbant ou désorganisant la société, en engendrant d'importantes pertes financières et en bouleversant le fonctionnement de notre économie.

Pour protéger ce secteur vital, un dispositif de cybersécurité spécifique au plan VIGIPIRATE est mis en place. Il concerne plusieurs acteurs :

- l'Agence nationale de la sécurité des systèmes d'information (ANSSI) organise et coordonne la mise en œuvre de la partie cybersécurité du plan VIGIPIRATE. Elle s'appuie sur le ministère coordonnateur de chacun des secteurs d'importance vitale concernés ;
- les opérateurs d'importance vitale (OIV)[22] appliquent les mesures de sécurité informatique propres à leur secteur et doivent aussi les faire appliquer de manière appropriée par leurs sous-traitants ;
- les administrations dans leur ensemble, en tant que responsables de systèmes d'information de l'Etat, mettent en œuvre les instructions du plan VIGIPIRATE qui leur incombent ;
- les collectivités territoriales et les opérateurs non-OIV sont incités à mettre en œuvre le plan VIGIPIRATE ;
- les citoyens qui, chaque jour, dans leur vie professionnelle ou privée, ont un rapport avec les systèmes d'information, sont invités à appliquer les règles essentielles de précaution et de vigilance.

Stratégie de sécurité

La stratégie consiste en une **posture permanente de sécurité (cybersécurité) ainsi qu'à intégrer les mesures de protection renforcée adaptées à l'évolution de la menace (cyberdéfense)**.

22- Pour plus de détails, voir le « *Glossaire* » page 73.

6. PROTÉGER LE SECTEUR AÉRIEN

Description du domaine

Le secteur aérien concerne **les activités qui protègent ou utilisent l'espace aérien national, l'ensemble des infrastructures qui leur sont associées, l'ensemble des aéronefs français et étrangers, les usagers et les professionnels du transport aérien.**

L'Etat est un acteur majeur de sa protection. Le ministre chargé des transports est l'autorité compétente en matière de sûreté de l'aviation civile. A ce titre, il est responsable de la coordination avec les autres administrations concernées, il élabore et anime la politique de l'Etat et veille à son application par les différents acteurs et opérateurs du transport aérien. Il représente le gouvernement dans les instances de concertation européennes et internationales.

La mise en œuvre des mesures de sûreté est de la responsabilité des acteurs privés (exploitants d'aérodrome, entreprises de transport aérien, agents habilités), la surveillance de cette mise en œuvre étant réalisée par le ministère chargé des transports, le ministère de l'Intérieur et le ministère chargé du budget.

Sous l'autorité directe du Premier ministre, l'armée de l'air assure la défense aérienne de l'espace aérien national et de ses approches. Cette mission consiste à y faire respecter la souveraineté et à s'opposer à son utilisation par un éventuel agresseur. Ce dispositif est complété par des accords bilatéraux avec les pays limitrophes.

Le plan VIGIPIRATE associe de nombreux acteurs au-delà du seul périmètre de l'Etat, qui ont à des degrés divers des obligations en matière de sûreté et de sécurité ou peuvent y contribuer. Ils peuvent faire l'objet de réglementations nationales ou de directives ou encore de recommandations spécifiques dans le cadre de la protection contre la menace terroriste. Il s'agit notamment des entreprises de transport aérien, des exploitants des aérodromes de métropole et d'outre-mer, des services de sûreté, des services à compétence nationale en matière de navigation aérienne, de météorologie.

Stratégie de sécurité

La stratégie vise à **protéger les usagers et les professionnels du transport aérien et des installations aéronautiques, l'espace aérien national ainsi que les aéronefs et d'assurer par ailleurs le niveau de vigilance requis dans les zones accessibles au public et aux professionnels des aéroports.**

L'objectif est d'assurer la meilleure cohérence possible de l'ensemble des mesures de protection relatives aux différentes composantes du secteur aérien, mais également de protéger les passagers, les accompagnants et les professionnels du secteur aérien.

7. PROTÉGER LE SECTEUR MARITIME

Description du domaine

Les espaces maritimes sous souveraineté française représentent près de 11 millions de km² répartis dans toutes les régions du monde. Le transport maritime concerne **les activités des navires et des infrastructures, ports, installations portuaires de soutien.**

La protection du secteur maritime associe différents acteurs. Les représentants de l'Etat (préfet maritime en métropole, préfet ou haut-commissaire de la République outre-mer) veillent à la souveraineté de la France sur ses espaces maritimes et coordonnent l'action des diverses administrations intervenant en mer. Le commandant de zone maritime est responsable de la mise en œuvre de la défense maritime du territoire. A ce titre, il assure une surveillance des approches.

Le plan VIGIPIRATE associe d'autres acteurs au-delà du seul périmètre de l'Etat, qui ont à des degrés divers des obligations en matière de sécurité ou peuvent y contribuer : les exploitants portuaires publics et privés dont les infrastructures assurent notamment la gestion de l'interface terre-navires, les responsables de la gestion de leurs navires, et toutes les activités dédiées à l'exploitation des navires et des ports.

Le transport maritime de marchandises représente 90% des échanges mondiaux et joue donc un rôle stratégique pour l'activité économique de la France. Ses principales vulnérabilités sont directement liées à la nature commerciale et à la dimension internationale de ses activités, ou encore à la nature de ses infrastructures : importance des flux de passagers et de marchandises, exigences de délai, nombre et banalisation des conteneurs, facilité d'accès aux installations portuaires, insertion des ports dans les villes et liberté de mouvement autour des navires.

Stratégie de sécurité

La stratégie vise à **protéger l'espace maritime des eaux territoriales, les navires, les zones réservées et les composants névralgiques des ports et installations portuaires, et à assurer le niveau de vigilance requis dans les zones publiques de ces ports.**

8. PROTÉGER LES TRANSPORTS TERRESTRES

Description du domaine

Le domaine des transports terrestres comprend **l'ensemble des moyens et organismes de transports collectifs et ferroviaires ainsi que les infrastructures linéaires de transports.**

Les infrastructures englobent non seulement les infrastructures physiques (routes, voies ferrées), mais également les systèmes d'information utilisés pour leur exploitation (signalisation, gestion du trafic, information des usagers, tarification) et les points d'échanges nodaux.

Le ministre chargé des transports assure la tutelle des différents acteurs du domaine qui concourent tous à sa protection à la mesure de leurs responsabilités, et qui sont essentiellement les gestionnaires d'infrastructures et les entreprises ayant une activité d'envergure nationale.

Stratégie de sécurité

La stratégie vise à **protéger les passagers dans les gares, dans les trains et dans les transports collectifs urbains. Elle vise également à protéger les composants névralgiques des infrastructures de transport terrestre** ainsi que certaines gares.

9. PROTÉGER LE SECTEUR DE LA SANTÉ

Description du domaine

Le secteur de la santé regroupe **l'ensemble des acteurs et des activités assurant l'offre de soins, la veille et la sécurité sanitaire, la production et la distribution des produits de santé, permettant de prévenir et, le cas échéant, d'assurer la prise en charge massive, y compris dans sa dimension médico-psychologique, de personnes, à la suite d'un acte terroriste (dont NRBC-E[23]).**

La protection du secteur associe divers acteurs. Le ministère de la Santé coordonne le fonctionnement du secteur via ses directions générales (direction générale de la santé, direction générale de l'offre de soins…) et par l'action des agences sanitaires (agences régionales de santé, agences nationales d'expertises). Les laboratoires de biologie médicale ou de toxicologie concourent également au dispositif de veille. Les entreprises pharmaceutiques ou les grossistes répartiteurs sont impliqués dans la sécurisation de l'approvisionnement des produits de santé. Enfin, les professionnels de santé libéraux constituent le premier maillon de la chaîne des soins, qui intègre une grande diversité d'établissements médico-sociaux publics ou privés.

Stratégie de sécurité

La stratégie vise :

- à **favoriser la généralisation de plans de sécurité interne dans les établissements de santé et les conventions « santé-sécurité-justice »** constitutifs d'une véritable posture permanente de vigilance et de sûreté dans le secteur de la santé ;
- à **adapter le dispositif de veille sanitaire et de sécurité sanitaire aux risques auxquels notre pays est confronté** ;
- à **sécuriser les capacités de production et de distribution d'une part des produits de santé**, mais aussi de **l'eau destinée à la consommation humaine**.

23- Voir « *Glossaire* » page 72.

10. PROTÉGER LA CHAÎNE ALIMENTAIRE

Description du domaine

La chaîne alimentaire est définie comme **l'ensemble des entreprises de production et de transformation et des centres de mise sur le marché de produits destinés à l'alimentation humaine ou animale.**

Aujourd'hui très fortement internationalisé, le secteur agro-alimentaire connaît une complexité croissante des systèmes de production, une évolution constante des modes d'approvisionnement ainsi que des développements technologiques constants. Il se caractérise par une grande diversité de filières comportant un grand nombre de petites entreprises au côté de grandes entreprises dont plusieurs multinationales.

Les filières essentielles comprennent :

- les **industries agroalimentaires,** représentant plus de 13 000 entreprises hors artisanat commercial, avec une place importante pour la transformation des produits de l'élevage ;
- la **grande distribution alimentaire** — 10 grands groupes nationaux — regroupant plus de 12 000 établissements en métropole.

Stratégie de sécurité

La stratégie vise à **favoriser la généralisation de plans de sécurité interne (PSI)[24]. Ces plans concernent six domaines : la protection physique des accès, le contrôle des flux de circulation (personnes, véhicules, produits), la sûreté liée au personnel de l'établissement, la gestion des stocks, les processus ainsi que la sûreté informatique.**

Dans les entreprises du secteur, ces plans sont constitutifs d'une véritable posture de vigilance et de sûreté permanentes. Ils peuvent, en outre, être modulés en fonction d'alertes et/ou de caractérisation plus précise de la menace.

24- Pour plus de détails, voir la rubrique « *Guides de bonnes pratiques* » page 71.

11. PROTÉGER LES RÉSEAUX

11.1. Protéger les réseaux de communications électroniques et de l'audiovisuel

Description du domaine

Le domaine des réseaux de communications électroniques et de l'audiovisuel comprend **l'ensemble des activités, des opérateurs et des installations assurant l'acheminement des communications électroniques,** c'est-à-dire les émissions, les transmissions ou les réceptions de signes, de signaux, d'écrits, d'images ou de sons par voie électromagnétique (fibre optique, câble, hertzien terrestre ou satellitaire). Il comprend la téléphonie fixe et mobile, les services de données fixes et mobiles, dont l'accès à Internet et les réseaux dits « sociaux » et la diffusion de programmes de télévision et de radio.

Deux acteurs contribuent à la protection du domaine :

- **le Commissariat aux communications électroniques de défense** (CCED), qui relève du ministre chargé des communications électroniques, veille à la satisfaction des besoins en communications électroniques liés à la défense et à la sécurité publique, ainsi qu'à l'application par les opérateurs des prescriptions législatives et réglementaires en matière de défense et de sécurité publique ;
- **l'Autorité de régulation des communications électroniques et des postes** (ARCEP) est l'autorité administrative indépendante chargée de réguler les communications électroniques en France.

Stratégie de sécurité

La stratégie vise à **éviter une interruption durable des communications électroniques.** Une attention particulière est portée aux dysfonctionnements et aux utilisations anormales des logiciels, car ils peuvent être d'origine malveillante. A cet égard, les objectifs de cybersécurité s'appliquent en totalité au domaine des communications électroniques.

11.2. Protéger les réseaux d'eau

Description du domaine

Ce domaine couvre l'ensemble des **activités de suivi sanitaire et de distribution de l'eau aux différents consommateurs publics et privés** dans le respect des règles du code de la santé publique. Il inclut les systèmes de pompage, de production, de stockage et d'alimentation en eau potable.

Le suivi sanitaire permanent des eaux destinées à la consommation humaine (EDCH) qui garantit la sécurité sanitaire comprend à la fois le contrôle sanitaire mis en œuvre par les agences régionales de santé (ARS) et la surveillance exercée par la personne responsable de la production ou de la distribution de l'eau (PRPDE). Le contrôle sanitaire, exercé en toute indépendance vis-à-vis des PRPDE, permet de vérifier le respect des dispositions législatives et réglementaires relatives à la sécurité sanitaire des EDCH. La surveillance concerne la vérification régulière des mesures prises pour protéger la ressource et celle du fonctionnement des installations, ainsi que la réalisation d'analyses en différents points.

Le service de production et de distribution de l'eau potable à la population relève de la compétence de la commune, du groupement de communes ou du syndicat d'alimentation en eau potable (maître d'ouvrage de ce service public). Ces instances ont la possibilité soit de gérer ce service en régie directe, soit de le déléguer par contrat d'affermage ou de concession (en fonction du degré de délégation) à une entreprise privée spécialisée.

Le service public de l'eau potable se distingue par la dispersion géographique sur l'ensemble du territoire national de plus de 25 000 unités de distribution d'eau potable (UDI, réseau ou partie du réseau physique de distribution qui délivre une eau de qualité réputée homogène, de même origine ayant le même propriétaire et le même exploitant). Ces UDI sont de taille diverse (allant de quelques dizaines de personnes alimentées à plusieurs centaines de milliers) et sont rarement interconnectées entre elles. Toutes les eaux distribuées ne sont pas traitées.

Stratégie de sécurité

La stratégie vise à **protéger les réseaux d'eau, à assurer le niveau de vigilance requis dans l'exploitation de ces réseaux, ainsi que d'assurer la permanence de la distribution.**

11.3. Protéger les réseaux d'électricité

Description du domaine

Ce domaine concerne **les activités permettant d'assurer la continuité de la distribution d'électricité à la population et à l'ensemble des activités.** Les trois fonctions principales du domaine sont la production d'électricité, son transport sur l'ensemble du territoire et en interconnexion avec d'autres pays, et sa distribution à l'ensemble des utilisateurs.

Plusieurs acteurs contribuent à la protection du domaine :

- la Commission de régulation de l'énergie (CRE) est l'autorité administrative indépendante chargée de veiller au bon fonctionnement des marchés de l'électricité et du gaz en France ;
- les services de l'Etat délivrent les autorisations d'exploitation sur avis de la CRE ;
- les opérateurs sont responsables de la continuité des services dont ils ont la charge : production, transport ou distribution.

Stratégie de sécurité

La stratégie vise à **maintenir la continuité des services en protégeant les réseaux d'électricité** et en assurant le niveau de vigilance requis dans leur exploitation.

11.4. Protéger les réseaux d'hydrocarbures

Description du domaine

Ce domaine concerne **l'importation, le raffinage, la distribution et la livraison des hydrocarbures liquides aux différents consommateurs publics et privés.** Toutes ces activités sont constituées en chaînes logistiques se reliant entre elles.

Plusieurs acteurs contribuent à la protection du domaine :

- les services de l'Etat (Direction générale de l'énergie et du climat, DGEC) décident de l'utilisation éventuelle des stocks stratégiques dans le cadre des accords liant les Etats adhérents à l'Agence internationale de l'énergie, conformément à la réglementation européenne ;
- les opérateurs du secteur pétrolier sont nombreux et de taille variable, et se répartissent selon leurs activités logistiques plus ou moins intégrées ;
- les grands opérateurs agissant en réseaux d'activités intégrées ;
- les opérateurs indépendants qui assurent quelques métiers pétroliers (distribution, stockage) ;
- les grandes et moyennes surfaces, qui détiennent 56% du marché des stations-service ;
- les distributeurs de fioul domestique.

Les défis de la protection de ce domaine sont liés à la sensibilité même des hydrocarbures stockés et transportés à travers les réseaux. La protection d'un certain nombre d'infrastructures relève du plan consacré aux installations et matières dangereuses. La protection des réseaux d'hydrocarbures porte surtout sur les composants névralgiques assurant le fonctionnement et la continuité des services de transport et de distribution.

Stratégie de sécurité

La stratégie vise à **maintenir la continuité des services en protégeant les réseaux d'hydrocarbures** et en assurant le niveau de vigilance requis dans leur exploitation.

11.5. Protéger les réseaux de gaz

Description du domaine

Ce domaine couvre **les activités de transport, de stockage et de distribution de gaz permettant d'assurer, à partir d'importations, la continuité de la fourniture aux différents consommateurs publics et privés,** soit par gazoduc, soit sous forme de gaz naturel liquéfié (GNL) à partir des terminaux méthaniers.

Plusieurs acteurs contribuent à la protection du domaine :

- la Commission de régulation de l'énergie (CRE) veille au bon fonctionnement des marchés de l'électricité et du gaz en France et à l'indépendance des gestionnaires ;
- les services de l'Etat délivrent les autorisations d'exploitation sur avis de la CRE ;
- les opérateurs sont responsables de la continuité du service dont ils ont la charge : transport, stockage ou distribution.

Stratégie de sécurité

La stratégie vise à **maintenir la continuité des services en protégeant les réseaux de gaz** et en assurant le niveau de vigilance requis dans leur exploitation.

12. CONTRÔLER LES FRONTIÈRES

Description du domaine

Ce domaine concerne **les frontières terrestres (routières et ferroviaires), y compris fluviales et lacustres, maritimes et aériennes sous souveraineté française.** La France compte 132 points de passage frontaliers (PPF), correspondant aux frontières externes, et a identifié au moins 285 points de passage autorisés (PPA) qu'elle peut activer aux frontières internes en cas de nécessité.

La mise en œuvre des mesures VIGIPIRATE de contrôle aux frontières s'applique dans deux cadres :

- **en action préventive :** certains points de passage peuvent être contrôlés en cas d'organisation d'un événement national nécessitant une protection renforcée ou en cas d'identification d'une menace grave et imminente pour l'ordre public ou la sécurité intérieure ;
- **en réaction à un attentat :** certains points de passage peuvent être contrôlés en cas d'attaque terroriste afin d'éviter la sortie du territoire des responsables ou l'entrée sur le territoire d'éventuels complices.

Plusieurs acteurs contribuent à la protection du domaine :

- les acteurs étatiques responsables du contrôle aux frontières : direction centrale de la police aux frontières et la direction générale des douanes et des droits indirects ;
- les acteurs étatiques intervenant en renfort : gendarmerie nationale, police nationale, armées, direction générale des infrastructures, des transports et de la mer, directions régionales de l'environnement, de l'aménagement et du logement ;
- les acteurs hors du périmètre de l'Etat : opérateurs aéroportuaires et portuaires, Commission européenne ainsi que les autres Etats européens, l'Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des Etats membres de l'Union européenne (Frontex).

Stratégie de sécurité

La stratégie de sécurité vise à **favoriser la planification interministérielle et organiser le déploiement des unités engagées dans la mission de contrôle aux frontières** dans le cadre de la lutte contre le terrorisme.

13. PROTÉGER LES RESSORTISSANTS ET LES INTÉRÊTS FRANÇAIS À L'ÉTRANGER

Description du domaine

Le domaine étranger du plan VIGIPIRATE **comprend tous les pays où la France est présente, qui hébergent ses ressortissants et sont susceptibles d'accueillir des voyageurs français.** La présence française inclut à la fois les emprises diplomatiques et consulaires, les formations militaires stationnées à l'étranger ou en opération, les militaires en coopération, les instituts culturels, les établissements scolaires, culturels et de recherche et les entreprises. La France assure la protection de ses ressortissants, qu'ils soient résidents ou de passage.

Sous l'autorité du Premier ministre, le ministère des Affaires étrangères et du Développement international définit et met en œuvre les mesures de sûreté qui s'appliquent aux postes diplomatiques et assure la coordination interministérielle en matière de sécurité des ressortissants et des intérêts français.

Le ministère des Affaires étrangères a autorité sur les missions diplomatiques. Elles sont le lieu de convergence de toutes les informations et capacités d'action en cas de menace à l'étranger. Elles apportent leur expertise sur chaque pays et assurent la liaison localement avec les ressortissants, avec le réseau des établissements d'enseignement, avec les entreprises, avec les autorités politiques locales et avec les représentations diplomatiques des autres pays.

D'autres ministères sont parties prenantes de la protection à l'étranger. Le ministère de la Défense est responsable de la définition et de la mise en œuvre des mesures de protection des formations militaires stationnées à l'étranger ou en opération, dans le cadre des accords pris avec les pays hôtes. Le ministère de l'Intérieur assure une mission permanente de protection et de sécurité dans un certain nombre de représentations diplomatiques. Le ministère chargé des transports participe à la protection du transport aérien et maritime à l'étranger, et assure la liaison avec les opérateurs concernés.

Les entreprises sont, quant à elles, responsables de la sécurité de leurs employés.

La menace terroriste à l'étranger est très diverse, tant par ses origines que par ses manifestations. Elle peut émaner d'organisations ou de réseaux plus ou moins indépendants à l'échelle locale ou internationale, voire d'individus isolés. Elle peut relever d'idéologies politiques et religieuses, de motivations criminelles ou mafieuses. Elle peut se manifester à la suite d'intentions clairement affichées ou par opportunité, en fonction des situations politico-économiques locales et des positions de politique étrangère de la France ou de ses alliés. Les modes d'action peuvent être extrêmement variés. Les cibles potentielles peuvent être regroupées en trois principales catégories : les ressortissants, les emprises représentatives de la France et les entreprises.

Stratégie de sécurité

Pour répondre à ces enjeux à l'étranger, le plan VIGIPIRATE vise à **protéger les résidents français, les personnes vulnérables, les voyageurs, le personnel de l'Etat, les aéronefs et les aérodromes qui les accueillent, les navires et les ports qui les accueillent.** Par ailleurs, il vise à **renforcer la vigilance autour des emprises représentatives de l'Etat et des entreprises françaises.**

EN SAVOIR PLUS

Les autres plans PIRATE

Les plans activés en cas d'attaque terroriste utilisant un moyen d'agression spécifique :

- le **plan NRBC** (nucléaire, radiologique, biologique ou chimique) prévoit les modalités d'intervention en cas de menace ou d'exécution avérée d'une action malveillante ou à caractère terroriste utilisant des matières, agents ou des produits NRBC ;
- le **plan PIRANET** permet d'intervenir en cas de crise d'origine informatique.

Les plans activés en cas d'attaque terroriste se déroulant dans un milieu particulier :

- le **plan PIRATAIR-INTRUSAIR** est un plan d'intervention qui vise à contrer des actes illicites avérés ou imminents en matière de sûreté aérienne (PIRATAIR) et de souveraineté aérienne (INTRUSAIR) ;
- le **plan PIRATE-MER** permet d'intervenir contre le terrorisme et la piraterie maritime et, plus généralement, contre tout acte de malveillance en mer pouvant être associé à une prise d'otages ;
- le **plan METROPIRATE** permet d'intervenir en cas d'attaque dans les transports collectifs ferrés souterrains.

Documentation

- ***Guide interministériel de prévention de la radicalisation***, document du Comité interministériel de prévention de la délinquance, mars 2016
- ***Livre blanc sur la défense et la sécurité nationale de 2008***, disponible en ligne sur : http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000341.pdf
- ***Livre blanc sur la défense et la sécurité nationale de 2013***, disponible en ligne sur : http://www.livreblancdefenseetsecurite.gouv.fr/
- ***Plaquette d'information contre la radicalisation, document du ministère de l'Intérieur (MI/SG/DICOM - 04/2015)***, disponible sur : http://www.interieur.gouv.fr/SG-CIPDR/Prevenir-la-radicalisation/Prevenir-la-radicalisation
- ***Arrêté du 17 décembre 2015*** relatif à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord
- ***Arrêté du 17 décembre 2015*** relatif à la conception des aéronefs civils qui circulent sans personne à bord, aux conditions de leur emploi et aux capacités requises des personnes qui les utilisent
- ***Plan d'action contre la radicalisation et le terrorisme du 9 mai 2916.***

Sites Internet

- 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

Plateformes de signalement :

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

Guides de bonnes pratiques

- ***L'ensemble des guides sectoriels de bonnes pratiques Vigipirate sont consultables sur le site Internet suivant :*** *http://www.encasdattaque.gouv.fr*
- ***Guide d'hygiène informatique destiné aux entreprises****, disponible sur le site http://www.ssi.gouv.fr/*
- ***Guide des recommandations pour la protection de la chaîne alimentaire contre les risques d'actions malveillantes, criminelles ou terroristes****, disponible sur le site http://agriculture.gouv.fr/sites/minagri/files/documents/pdf/guide-2014_140214_V2*

Application SAIP

Plus d'informations sur le site : http://www.gouvernement.fr/appli-alerte-saip

Pour la télécharger, rendez-vous sur : http://appstore.com

GLOSSAIRE

ANSSI Agence nationale de la sécurité des systèmes d'information. Rattachée au SGDSN, chargée de la protection et de la prévention face à la cybermenace, elle organise et coordonne la mise en œuvre de la partie cybersécurité du plan VIGIPIRATE.

ARCEP L'Autorité de régulation des communications électroniques et des postes est l'autorité administrative indépendante chargée de réguler les communications électroniques en France.

CCED Le Commissariat aux communications électroniques de défense relève des ministères économiques et financiers, et veille à la satisfaction des besoins en communications liés à la défense et à la sécurité publique.

CIAV La Cellule interministérielle d'aide aux victimes centralise en temps réel l'ensemble des informations concernant l'état des victimes, informe et accompagne leurs proches et coordonne l'action de tous les ministères intervenants, en relation avec les associations et le parquet. Elle est placée sous l'autorité du Premier ministre qui décide de son activation et de sa fermeture.

CNR Coordonnateur national du renseignement, placé auprès du Président de la République, il coordonne l'action des services de renseignement et s'assure de leur bonne coopération.

CRE La Commission de régulation de l'énergie est l'autorité administrative indépendante chargée de veiller au bon fonctionnement des marchés de l'électricité et du gaz en France.

FGTI Le Fonds de garantie a pour mission l'indemnisation des victimes au titre de la solidarité nationale et exerce des actions de recours contre les responsables de dommages.

Frontex Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des Etats membres de l'Union européenne, elle a pour mission de coordonner la coopération opérationnelle des Etats membres aux frontières extérieures de l'Union européenne en matière de lutte contre l'immigration clandestine.

ISPS Code international pour la sûreté des navires et des installations portuaires.

NRBC Nucléaire, radiologique, biologique et chimique. Terminologie générique utilisée pour désigner les armes non conventionnelles ou les risques technologiques dont les effets sont difficiles à contrôler et à confiner en raison de leur puissance ou de leur pouvoir de dissémination dans l'environnement.

Objectif de sécurité Effet à obtenir en termes de vigilance et de protection pour contrer les menaces et réduire les vulnérabilités dans un domaine d'activité particulier.

OIV Certains opérateurs sont dits d'importance vitale lorsque leur secteur d'activité a un caractère soit « *difficilement substituable et remplaçable à la production de biens ou de services indispensables, soit peuvent présenter un danger grave pour la population* ». Ces services doivent être indispensables à la satisfaction des besoins essentiels pour la vie des populations, à l'exercice de l'autorité de l'Etat, au fonctionnement de l'économie, au maintien du potentiel de défense ou à la sécurité de la Nation.

Résilience Le Livre blanc de 2008 définit la résilience « *comme la volonté et la capacité d'un pays, de la société et des pouvoirs publics à résister aux conséquences d'une agression ou d'une catastrophe majeure, puis à rétablir rapidement leur capacité de fonctionner normalement, ou tout le moins dans un mode socialement acceptable. Elle concerne non seulement les pouvoirs publics, mais encore les acteurs économiques et la société civile toute entière.* »

SAIP Système d'alerte et d'information des populations. A la suite des attentats survenus en France en janvier et novembre 2015, et à la demande du Premier ministre, le ministère de l'Intérieur et le Service d'information du Gouvernement lancent une application mobile d'alerte sur smartphone : SAIP, le Système d'alerte et d'information des populations.

SAIV Sécurité des activités d'importance vitale. Dispositif de sécurité qui donne un cadre juridique spécifique aux opérateurs d'importance vitale pour les faire coopérer à la protection de leurs installations critiques contre toute menace, notamment à caractère terroriste.

SIG Service d'information du Gouvernement, direction des services du Premier ministre, placée sous l'autorité directe de celui-ci. Il analyse l'évolution de l'opinion publique et le traitement médiatique de l'action gouvernementale ; il informe le grand public de l'action du Premier ministre et du Gouvernement et pilote et coordonne au niveau interministériel la communication gouvernementale.

SGDSN Secrétariat général de la défense et de la sécurité nationale, service du Premier ministre chargé notamment du pilotage du plan VIGIPIRATE.

SHFDS Service du haut fonctionnaire de défense et de sécurité. Il appartient à la haute fonction publique. Placé auprès du ministre, il anime et coordonne la politique en matière de défense, de vigilance, de prévention de crise et de situation d'urgence.

UCLAT Unité de coordination de la lutte antiterroriste. Placée sous la responsabilité du ministre de l'Intérieur, elle assure une coordination des différents services chargés de la lutte contre le terrorisme.

NUMÉROS UTILES

En cas d'attaque ou pour signaler une situation anormale

17

112

114 (pour les personnes ayant des difficultés à entendre ou à parler)

Dans un train ou un transport collectif

31 17

ou

SMS 31 177

ou

application Alerte 3117

En cas d'attaque avec un produit toxique

15 (SAMU)

18 (pompiers)

112

114 (pour les personnes ayant des difficultés à entendre ou à parler)

Victime d'un acte terroriste

15 (SAMU)

08 842 846 37 (*7* jours sur *7*)

Effectuer un signalement

Numéro vert

0 800 005 696

Crédit photos et illustrations : Service d'information du Gouvernement, ministère de l'Intérieur, ministère de l'Environnement, de l'Energie et de la Mer, ministère de l'Economie et des Finances, ministère des Affaires sociales et de la Santé, ministère de l'Agriculture.

NOTES

VIGIPIRATE

FAIRE FACE ENSEMBLE

VIGILANCE, PRÉVENTION ET PROTECTION FACE À LA MENACE TERRORISTE

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

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

Maquette et impression : Pôle Conception graphique-Fabrication – DSAF/DPL – Novembre 2016.