PREMIER
MINISTRE

Liberté
Égalité
Fraternité

FAIRE FACE ENSEMBLE

VIGIPIRATE

VIGILANCE, PRÉVENTION ET PROTECTION FACE À LA MENACE TERRORISTE

Secrétariat général de la défense et de la sécurité nationale

PRÉFACE

La sécurité nationale a pour finalité d'assurer aux Français une protection efficace face à l'ensemble des risques et des menaces susceptibles d'avoir un impact majeur sur le fonctionnement du pays, de garantir la continuité des fonctions vitales de la Nation et de renforcer sa résilience.

Les missions fondamentales de l'État demeurent inchangées mais l'évolution rapide de l'environnement international, l'accumulation des facteurs d'instabilité et de crises modifient profondément la nature, la fréquence et l'intensité des risques et menaces auxquelles la France est confrontée.

Dans ce contexte, la revue nationale stratégique (RNS) de juillet 2025 fixe un cap clair : se préparer selon un scénario central combinant, d'une part, des actions déstabilisatrices de nature hybride visant notre cohésion et notre capacité de décision, et, d'autre part, la participation à une guerre majeure au-delà de nos frontières. Ce scénario central traduit le retour du recours désinhibé à la force comme mode de règlement des différends entre États.

Face à ces risques et à ces menaces de nature à entraver la liberté d'action de la France, l'élaboration d'un nouveau plan national s'est imposée. Le plan de défense et de sécurité national (PDSN), élaboré par le Secrétariat général de la défense et de la sécurité nationale (SGDSN) en lien avec l'ensemble des ministères, devient ainsi un référentiel complémentaire de la défense et de la sécurité nationale. Il vise à préparer l'ensemble de la Nation à l'appui de ses forces armées, à renforcer la continuité des fonctions essentielles et à mettre en place des mécanismes de lutte contre les stratégies hybrides conduites contre notre pays et qui cherchent la désorganisation politique et sociale et l'affaiblissement de la cohésion nationale.

Pour autant, ce nouveau contexte, comme les outils mis en place pour y répondre, n'atténuent en rien la menace terroriste, qui demeure élevée et durable. En conséquence, le plan VIGIPIRATE rénové acte un recentrage explicite sur cette menace, le volet cyber relevant désormais du PDSN.

Dans une logique de continuum entre sécurité intérieure et sécurité extérieure, le plan VIGIPIRATE rénové permet d'appréhender et de combattre la menace terroriste selon le triptyque historique : vigilance, prévention et protection. Il constitue à la fois un cadre de compréhension des enjeux, un outil d'aide à la décision et un instrument de conduite opérationnelle, destiné à assurer la préparation et la réaction de l'ensemble des acteurs publics comme privés, face à la menace ou la commission d'actes terroristes.

Cette ambition se traduit dans la structure même du plan rénové, qui comprend, comme son prédécesseur, deux volets complémentaires : un document public, « Faire face ensemble », destiné à mobiliser la communauté nationale — notamment autour d'une identité visuelle renouvelée — et un document classifié, destiné aux administrations et aux opérateurs d'importance vitale (OIV).

VIGIPIRATE est également rénové dans la gestion des différentes postures afin de rendre le plan plus agile. Ainsi, il instaure une période d'activation du niveau d'alerte sommital de 12 jours, au terme de laquelle la posture revient d'office au niveau d'alerte intermédiaire ou peut être renouvelée pour 12 jours, sur décision du Premier Ministre.

Qu'il s'agisse de la lutte contre le terrorisme, de la réponse aux stratégies hybrides dirigées contre la France ou de l'appui de la Nation à ses armées, l'engagement de chacune et de chacun demeure la condition fondamentale de notre sécurité nationale.

SOMMAIRE

PARTIE 2 : TOUS IMPLIQUÉS 19

INTRODUCTION

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

La menace terroriste, quelle que soit son inspiration, n'a pas disparu. Elle reste prégnante et durable et vise tout à la fois le territoire national ou nos ressortissants et intérêts à l'étranger. Pour y faire face, la France dispose d'un dispositif national complet et très structuré, 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'État, les collectivités territoriales, les opérateurs publics et privés et les citoyens - à une démarche de vigilance, de prévention et de protection.

VIGIPIRATE : à la fois plan national et dispositif de sécurité

L'État 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'État 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 qui peuvent être distinguées 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'État. En cas de crise majeure, ils facilitent la coordination de l'ensemble des acteurs concernés, au premier rang desquels figurent les différents ministères.

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, PIRATE mobilité terrestre.

Architecture et fonctionnement du plan VIGIPIRATE

Le plan VIGIPIRATE comprend 249 mesures s'appliquant aux 9 activités clés de la Nation et aux 6 fonctions de coordination de la gestion de crise utiles au plan. Ces mesures sont réparties entre un socle de mesures permanentes et un ensemble de mesures additionnelles, 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 terroristes.

Ces postures sont diffusées :

- périodiquement, en fonction de l'état de la menace et des grands événements du pays ;
- dans le cadre de grands événements nationaux (JOP 24 par exemple) ;
- après un attentat, sur le territoire national ou à l'étranger, afin d'adapter au mieux le dispositif national de protection.

Cette démarche repose sur trois grands principes :

1. l'analyse croisée de la menace et des vulnérabilités ;
2. une organisation des actions par activités clés ou fonctions de coordination, en identifiant les leviers d'action adaptés à l'intensité de la menace pour réduire les vulnérabilités des grands secteurs nationaux ;
3. une approche par objectifs de sécurité permettant de choisir les mesures les plus adaptées et leurs modalités de mise en application.

La menace terroriste se maintient durablement à un niveau élevé

Qu'est-ce que le terrorisme ?

La France, dans son Livre blanc sur la défense et la sécurité nationale (LBDSN) 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 ».

L'intensité de cette menace terroriste est précisée dans la directive générale interministérielle (DGI) n° 320 de 2023 qui précise que « la France est confrontée à un niveau de menace à l'intensité durablement élevée, émanant de groupes extrémistes de toutes natures. À la fois diffuse et omniprésente, agissant à l'extérieur comme à l'intérieur du territoire national, cette menace est ponctuée de pics de crise constitués par les attaques majeures ».

D'un point de vue légal, le code pénal (article 421-1) précise par ailleurs que le terrorisme « a pour but de troubler gravement l'ordre public par l'intimidation ou la terreur ». En France, seul le parquet national antiterroriste (PNAT) est compétent pour qualifier, juridiquement, dans le temps de la flagrance, un acte de terroriste.

De la menace d'inspiration djihadiste à la menace terroriste globale

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 ampleur mondiale suite aux attentats du 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.

Ainsi, la revue nationale stratégique (RNS) de 2025 met en exergue « l'instabilité au Levant, et notamment l'incertitude en Syrie, [qui] a remis le terrorisme djihadiste au premier rang des menaces non-étatiques visant la France. La menace persistante de Daech et d'attaques terroristes en France et en Europe est désormais majeure ».

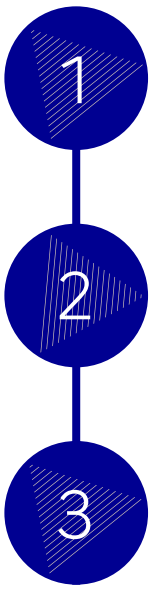
Au-delà de cette menace principale, des menaces terroristes historiques refont surface : mouvements d'ultras (ultra gauche, éco-terroristes, etc.) et mouvements séparatistes (groupes régionalistes français). D'autres menaces apparaissent comme celles issues de la mouvance incel.

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, notamment à Paris 2015 et à Nice 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.

Bien qu'évolutifs et s'adaptant en permanence aux évolutions de la technique et des modes de vie, les modes opératoires suivants perdurent :

- 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 ou biologiques;
- 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.

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.).

LE PLAN VIGIPIRATE

1 PRINCIPES ET OBJECTIFS

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

Le plan VIGIPIRATE repose sur trois piliers :

VIGILANCE

la **vigilance** qui 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 ;

PRÉVENTION

la **prévention** qui 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 ;

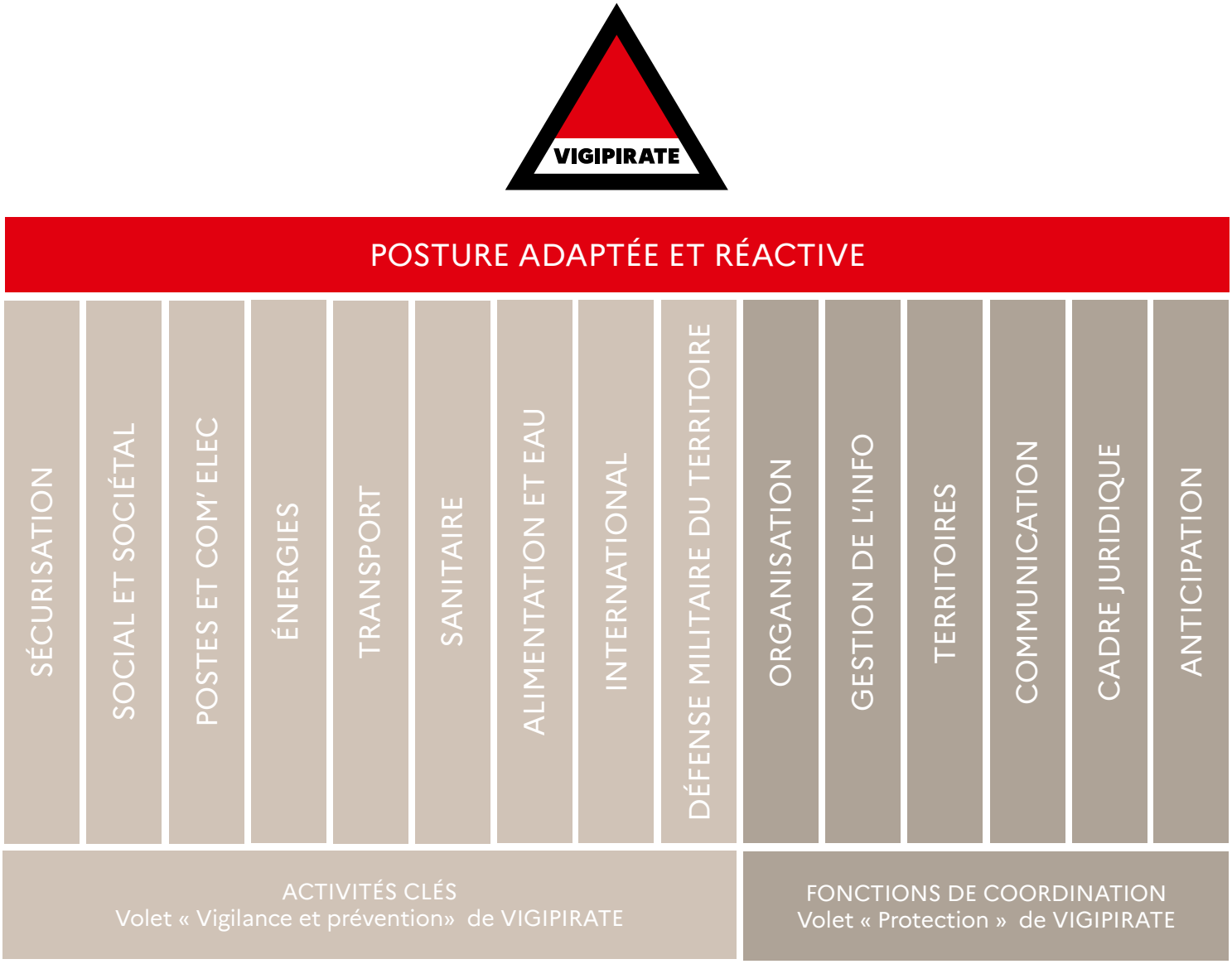
PROTECTION

enfin, la **protection** qui 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.

Le plan est structuré en 9 activités clés et 6 fonctions de coordination. Une activité clé est constituée par une ou plusieurs sous-activités et identifie une famille d'objectifs de sécurité. Il en va de même pour les fonctions de coordination qui décrivent des sous-fonctions utiles à la gestion de crise. Sont explicités au sein des différentes activités clés ou fonctions de coordination :

- les caractéristiques, les enjeux et les acteurs ;
- les objectifs de sécurité propres à l'activité clé ou à la fonction de coordination ;
- 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.



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 intitulée « Faire Face Ensemble » et une partie classifée [SECRET].

Cette partie publique du plan est un outil pédagogique, accessible à tous, qui contribue à développer une culture de sécurité collective. Elle permet aux entreprises publiques et privées, aux collectivités territoriales, ainsi qu'à chacun des citoyens de comprendre le fonctionnement du plan VIGIPIRATE.

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 [SECRET] du plan VIGIPIRATE comprend deux volets :

- le corps du plan qui détaille la stratégie, les objectifs et les mesures pour l'ensemble des activités clés et fonctions de coordination ;

- le corpus des fiches mesures du plan qui est stocké sur le logiciel de gestion interministérielle des crises ATHENA.

La partie publique du plan VIGIPIRATE comprend :

- un document de présentation du plan VIGIPIRATE et de conseils de comportement, destiné à l'ensemble des citoyens.

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'État les différentes catégories d'acteurs qui représentent des cibles potentielles pour les terroristes.

2.1 L'État

PREMIER MINISTRE

Le Premier ministre décide la mise en œuvre des dispositions et des mesures prévues par le plan gouvernemental VIGIPIRATE.

SGDSN

Le SGDSN, rattaché directement au Premier ministre, assure le pilotage du plan VIGIPIRATE.

MINISTRE DE L'INTÉRIEUR

Le ministre de l'Intérieur, responsable de la sécurité intérieure, de l'ordre public, de la protection des personnes, 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.

MINISTRE DES ARMÉES

Le ministre des armées est responsable de l'engagement des forces armées dans les milieux terrestre, aérien, et maritime dans le cadre de la manœuvre globale du gouvernement de lutte antiterroriste sur le territoire national.

MINISTRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Le ministre de l'Europe et des affaires étrangères 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.

MINISTRES

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.

PRÉFETS DE DÉPARTEMENT ET PRÉFETS MARITIMES

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

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 les préfets, 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 (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 (SAIV), mais aussi par le plan VIGIPIRATE.

D'une manière générale, toutes les entreprises publiques et privées doivent veiller à leur propre sécurité et 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 Les 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 de l'Europe et des affaires étrangères 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 États hôtes.

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 validées par le Premier ministre puis déclinées et diffusées par toute la chaîne ministérielle et préfectorale.

Ces postures sont préparées par le SGDSN, en étroite coordination avec les services de hauts fonctionnaires de défense et de sécurité (SHFDS) de l'ensemble des ministères. Elles sont actualisées périodiquement ou dans le cadre de la préparation des grands événements nationaux (JOP 2024 par exemple) ou après un attentat.

La mise en œuvre du plan VIGIPIRATE combine trois démarches :

EVALUER

évaluer la menace terroriste en France et à l'encontre des ressortissants et intérêts français à l'étranger ;

CONNAÎTRE

connaître les vulnérabilités des principales cibles potentielles d'attaque terroriste afin de les réduire et de limiter préventivement les effets d'une telle attaque ;

DÉTERMINER

déterminer un dispositif de sécurité répondant au niveau de risque qui résulte du croisement des vulnérabilités avec l'état de la menace.

3.1 Évaluer 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 la coordination nationale du renseignement de la lutte contre le terrorisme (CNRLT).

La CNRLT fournit une évaluation de façon régulière, en fonction de l'actualité, de la menace terroriste. 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

L'identification des vulnérabilités et des risques par le plan VIGIPIRATE s'appuie sur les 9 activités clés de la Nation et les 6 fonctions de coordination décrites dans la direction générale interministérielle (DGI) n°320 déclinées dans le plan.

La continuité de la vie de la Nation dépend de la préservation des activités clés. Chaque activité clé fait l'objet d'une stratégie de sécurité spécifique fondée sur ses vulnérabilités propres qui vise à maintenir la continuité de l'activité, qu'elle soit concernée par l'origine de la crise ou qu'elle en affronte les conséquences à titre collatéral.

L'ensemble, activités clés et fonctions de coordination interministérielles, permet de proposer une grille d'analyse facilitant la réponse à tous les risques et l'intégration éventuelle de nouveaux enjeux.

Chaque objectif de sécurité s'appuie sur des mesures opérationnelles qui sont de deux types :

- 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 sont détaillées dans des fiches d'aide à la mise en œuvre, dénommées fiches mesures, faisant partie du volet classifié [SECRET] du plan.

3.3 Adopter 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 adoptées 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 protégé 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.

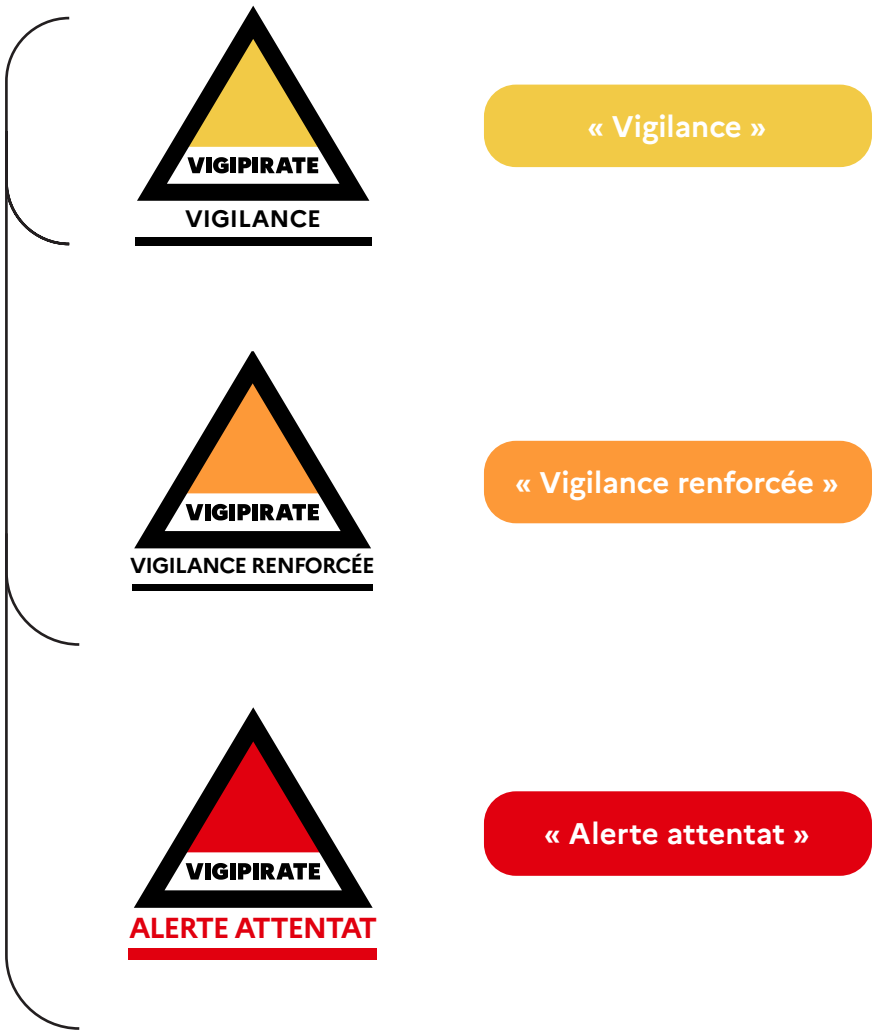
3.3.1 Le niveau d'alerte VIGIPIRATE

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 concerne le territoire métropolitain et les territoires ultramarins.

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.

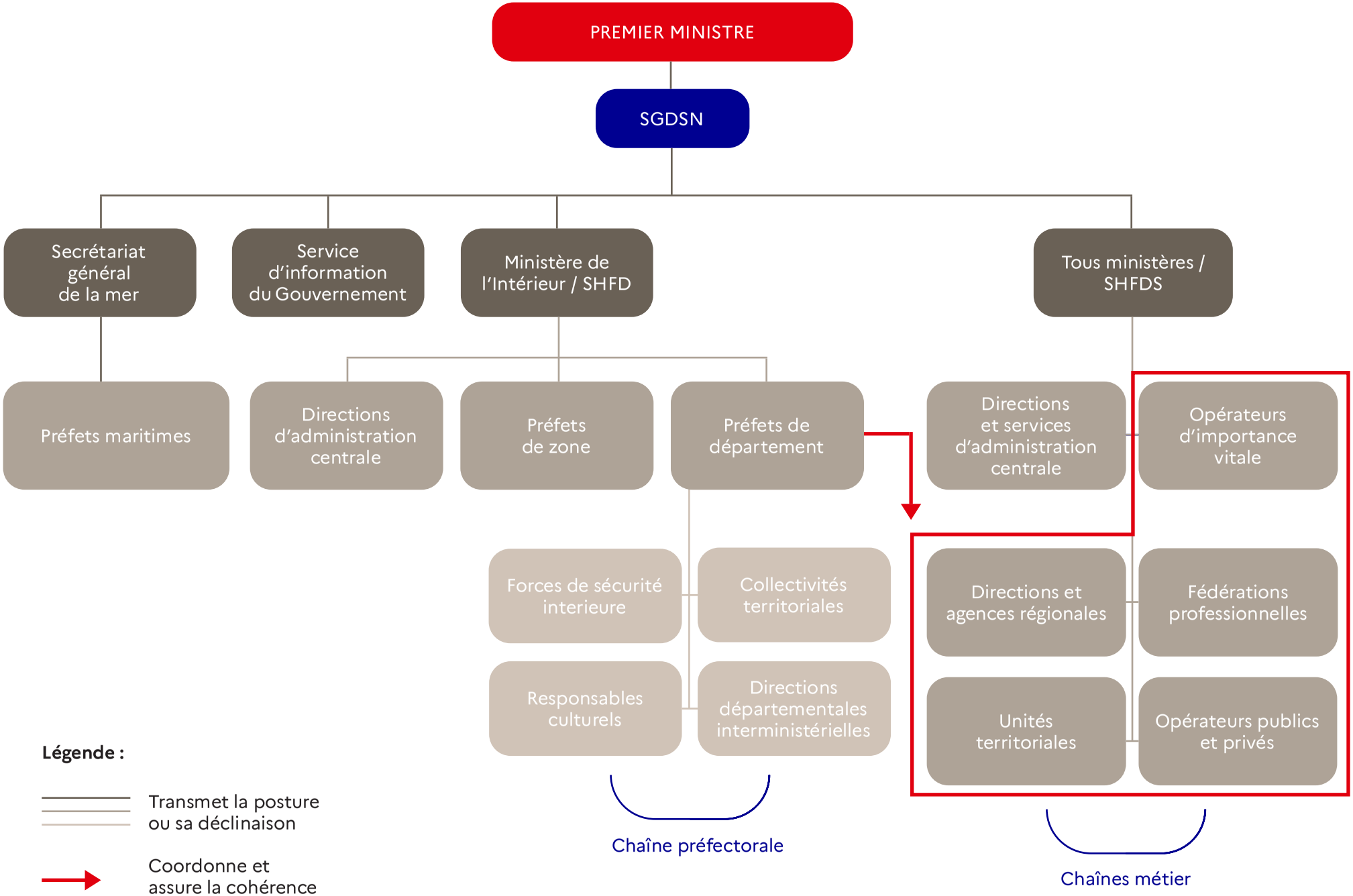
Le dispositif choisi doit être strictement dimensionné à l'évaluation de la menace.

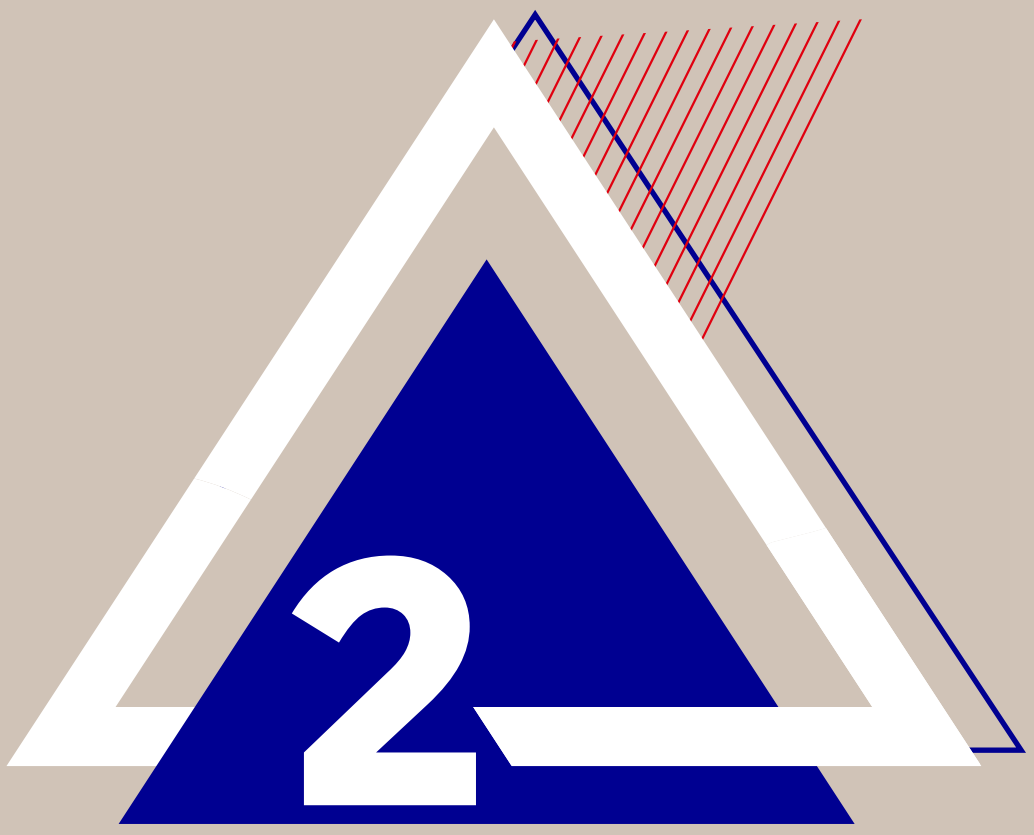
Trois niveaux sont distingués :



3.3.2 Diffusion des instructions relatives à la posture VIGIPIRATE

Conformément aux instructions données par le Premier ministre, chaque ministère donne des instructions dans son champ de compétence propre. De par la nature de sa mission et par l'intermédiaire des préfets, de la police nationale, de la gendarmerie nationale et de la sécurité civile, le ministère de l'intérieur joue un rôle prépondérant sur le territoire national. 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.


PREMIER MINISTRE
SGDSN
Secrétariat général de la mer
Service d'information du Gouvernement
Ministère de l'Intérieur / SHFD
Tous ministères / SHFDS
Préfets maritimes
Directions d'administration centrale
Préfets de zone
Préfets de département
Directions et services d'administration centrale
Opérateurs d'importance vitale
Forces de sécurité interieure
Collectivités territoriales
Responsables culturels
Directions départementales interministérielles
Directions et agences régionales
Fédérations professionnelles
Unités territoriales
Opérateurs publics et privés
Chaîne préfectorale
Chaînes métier
Légende :
Transmet la posture ou sa déclinaison
Coordonne et assure la cohérence



TOUS IMPLIQUÉS

SE PRÉPARER

4.1 Citoyen, que puis-je faire ?

4.1.1 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.

Être 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.

Être attentifs aux autres et à son environnement

4.1.2 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.

▶ 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.

▶ 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[1].

▶ Préparer ses voyages à l'étranger

Avant chaque voyage à l'étranger :

- consultez le site https://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://fildariane.diplomatie.gouv.fr/fildariane-internet/accueil 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] Consultez la liste des associations agréées : https://www.info.gouv.fr/risques/aider#se-former-aux-premiers-secours

4.2 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'État 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[2] 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.

4.2.1 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.

▶ Développer ses relations avec les partenaires extérieurs

La première des mesures de préparation est d'établir un réseau de sécurité. Les différents partenaires extérieurs sont les suivants :

- 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 et procèdent aux aménagements 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.

[2] https://www.sgdsn.gouv.fr/vigipirate/les-fiches-de-recommandations-et-de-bonnes-pratiques

▶ Analyser les vulnérabilités de son établissement

La deuxième étape est l'analyse des vulnérabilités de sa structure, en s'appuyant sur les analyses des acteurs mentionnés supra et sur la géographie du site considéré :

- 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).

▶ S'organiser

Très concrètement s'organiser signifie :

- **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 :**

  ▶ alertez 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, mettez 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 ».

  ▶ préparez :

  - 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.

▶ sensibilisez le personnel :

- informez 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 38)*. 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.

▶ formez 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.

4.2.2 Préparer un rassemblement

La sécurité d'un événement ne s'improvise pas. Faites-vous conseiller par des professionnels et consultez le guide des bonnes pratiques sur le site du SGDSN. Pour se préparer à un rassemblement de personnes, il faut :

▶ Identifier les menaces et les vulnérabilités

Évaluer la sensibilité du rassemblement en lien avec les services de l'État. 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.

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 vidéoprotection 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 vidéoprotection 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.

4.2.3 Réaliser des exercices progressifs

Les exercices de réaction à une attaque 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.

Voici quelques suggestions d'exercices progressifs :

- rappel simple des procédures et du rôle de chacun par le responsable du site ou son chargé de sûreté ;
- 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) ;
- test technique du système d'alerte ;
- organisation de reconnaissances exploratoires (lieux d'évacuation, salles de confinement, etc.) ;
- 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.

5 PRÉVENIR

5.1 Identification et signalement des phénomènes de radicalisation

La radicalisation est un processus progressif par lequel un individu ou un groupe adopte des idéologies extrêmes — souvent politiques, religieuses ou idéologiques — qui justifient l'usage de la violence pour imposer des changements sociaux, politiques ou religieux.

La radicalisation est un processus individuel non linéaire de rupture et de métamorphose, fondé sur trois critères :

- un changement inquiétant de comportement ;
- l'adhésion à une idéologie extrémiste ;
- l'adoption au moins en théorie de la violence comme mode d'action ou la légitimation/apologie de cette violence.

5.1.1 Pourquoi signaler un cas de radicalisation ?

La radicalisation concerne tout type d'idéologie extrémiste 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 extrémiste marquée par 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, y compris psychopathologiques. Certains groupes terroristes cherchent ainsi à enrôler des individus en perte de repères et vulnérables.

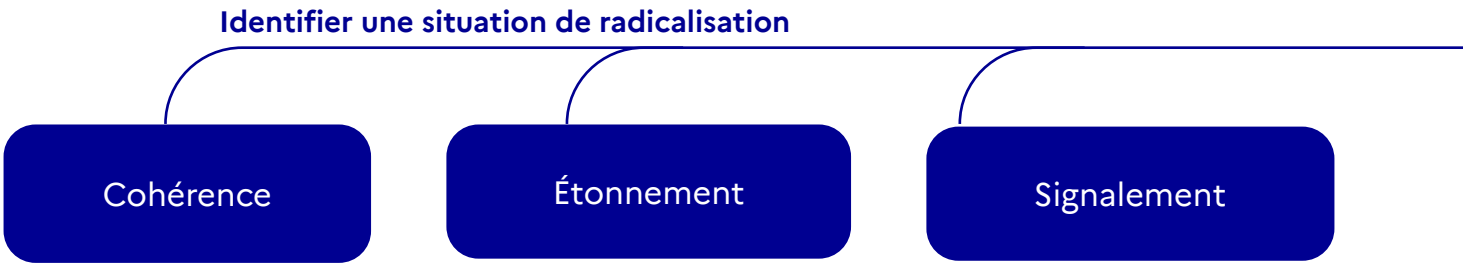
La force d'une idéologie extrémiste et son pouvoir d'attraction ne doivent pas être sous-estimés. Des individus ayant développé une haine de notre société peuvent adhérer pleinement à un discours qui donne sens à leur basculement dans la violence.

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 psychopathologiques, etc. Difficile à repérer et à contrer, la radicalisation est donc un enjeu majeur de sécurité nationale.

5.1.2 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 constituent des signaux forts de radicalisation et doivent attirer votre attention[3], que ce soit dans votre environnement quotidien, y compris familial, ou sur votre lieu de travail.



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.

Environnement personnel de l'individu :

- une image 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.

Théorie 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 ».

[3] *Guide interministériel de prévention de la radicalisation*, document du Comité interministériel de prévention de la radicalisation (CIPDR), mars 2016.

Les techniques :

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

5.1.3 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 leurs familles par des cellules spécialisées 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 surtout de protéger la population de possibles comportements violents[4].

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.

Que se passe-t-il après un signalement ?

Si la situation est jugée préoccupante par les services de l'État, 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 signes de radicalisation, vous pourriez sauver des vies. Il est donc préférable d'appeler rapidement le numéro vert. Des spécialistes se chargeront de lever le doute.

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 :
https://www.dgsi.interieur.gouv.fr/nous-contacter-radicalisation

5.2 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.

5.2.1 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

[4] *Guide interministériel de prévention de la radicalisation*, document du Comité interministériel de prévention de la radicalisation (CIPDR), mars 2016.

sécurité mises en place afin de les contourner, les chemins d'accès, etc. À 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

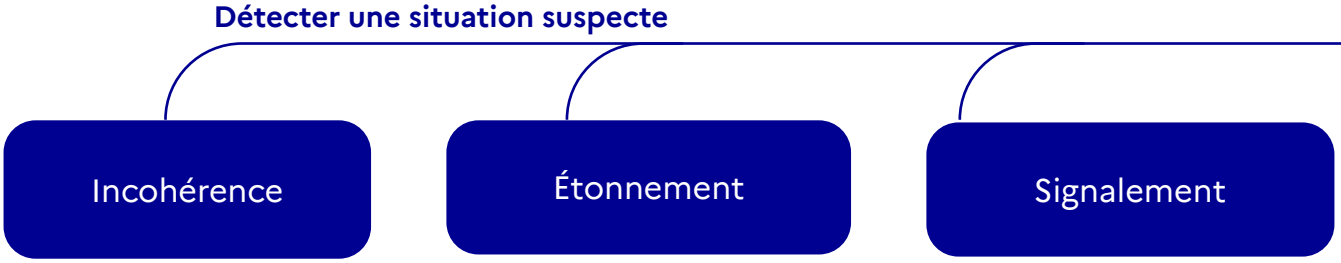
5.2.2 Comment détecter une situation suspecte ?

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.).



Comment une action terroriste est-elle planifiée ?

Comprendre la manière dont se planifie une action terroriste 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.

Le choix des cibles

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

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, film ou drone) 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.

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.

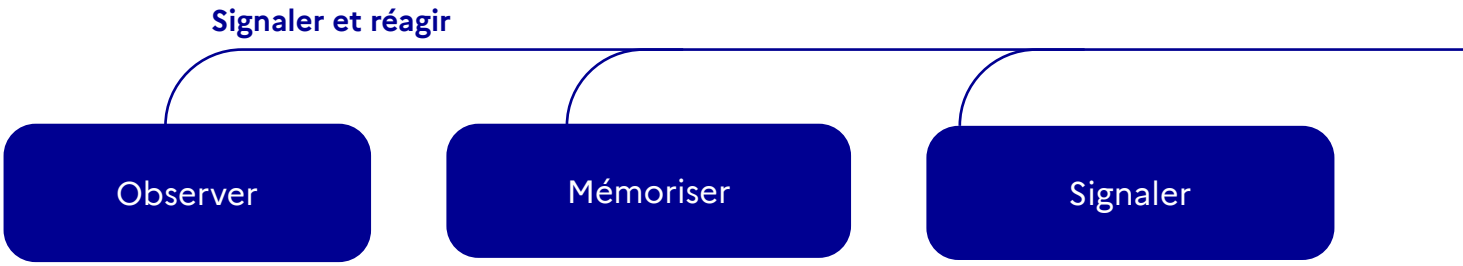
Une attaque à l'explosif peut également être réalisée. Certaines situations doivent vous alerter :

- 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.

5.2.3 Comment signaler et réagir ?

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.



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.

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[5], 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.

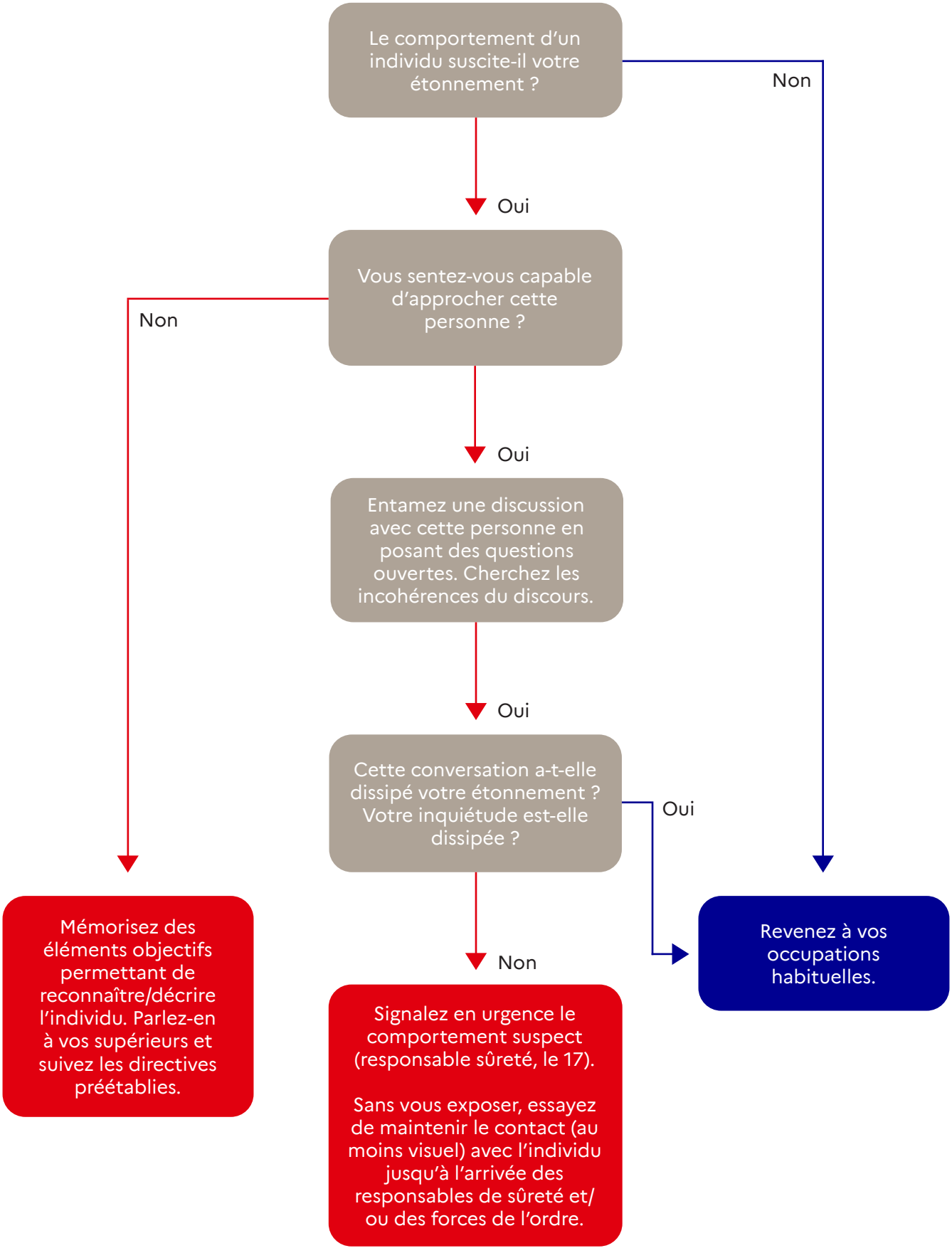
Par exemple, si un individu inconnu est repéré à l'intérieur d'une zone non ouverte au public, l'employé pourrait demander qui cette personne souhaite rencontrer. De même, si un individu prend des photos laissant penser à une reconnaissance, l'employé peut demander ce qui suscite l'intérêt de l'individu.

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.

[5] *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



5.2.4 Que faire en cas de survol de drones ?

Devenus accessibles et simples à mettre en œuvre, les drones constituent une menace sérieuse et en plein essor compte tenu des innovations importées depuis les théâtres de guerre. En effet, des personnes malveillantes peuvent utiliser ces nouveaux modes d'action pour collecter des informations en vue de la préparation ou de la conduite d'un acte terroriste. De plus, un drone peut représenter une arme du fait de sa capacité d'emport (grenade, arme chimique ou biologique, etc.), voire une arme par destination.

▶ Qu'est-ce qu'un drone malveillant ?

Les aéronefs civils circulant sans personne à bord, communément appelés drones, sont régis par l'arrêté du 3 décembre 2020[6]. En vertu de ce dernier, 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 sans déclaration préalable auprès des préfectures.

Ainsi, un drone survolant à proximité d'un site sensible, d'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[7] ».

▶ 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.

▶ 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.

[6] *Arrêté du 3 décembre 2020 relatif à l'utilisation de l'espace aérien par les aéronefs sans équipage à bord.*

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

6 RÉAGIR

6.1 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), des armes par destination (voitures bélier, camions, etc.) 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.

6.1.1 Cas général

Déterminez la réponse la plus appropriée à la situation. Celle-ci n'est pas figée et 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.

▶ 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.

S'enfermer, se cacher :

- 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.

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 !

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 :

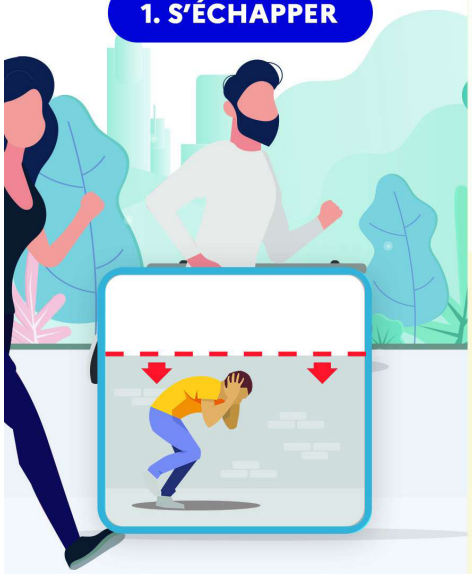
- distrayez l'adversaire (criez) et attaquez ;
- profitez d'un moment de vulnérabilité de l'agresseur (changement de chargeur, etc.) ;
- jetez des objets / utilisez des armes improvisées.

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

PREMIER MINISTRE
Liberté
Égalité
Fraternité

Réagir en cas d'attaque

1. S'ÉCHAPPER

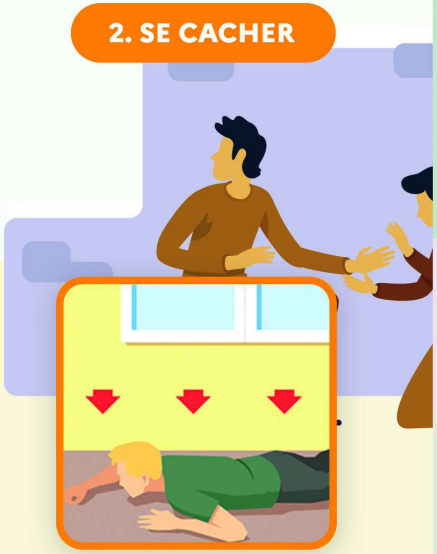


ÊTES-VOUS CERTAIN DE POUVOIR VOUS ÉCHAPPER SANS RISQUE ?

SI OUI

- Ne déclenchez pas l'alarme incendie
- Laissez toutes vos affaires sur place
- Ne vous exposez pas (courbez-vous)
- Prenez la sortie la moins exposée
- Utilisez un itinéraire connu
- Aidez les autres personnes à s'échapper
- Prévenez / alertez les personnes
- Évitez les mouvements de panique
- Facilitez l'intervention des forces de sécurité intérieure et des services de secours.

2. SE CACHER



SI NON ENFERMEZ-VOUS ET BARRICADEZ-VOUS

- Enfermez-vous et barricadez-vous
- éloignez-vous de la fenêtre
- Mettez les portables sur silencieux et décrochez les téléphones fixes
- Rassurez vos collègues
- Restez le plus silencieux et discret possible

3. ALERTER

UNE FOIS CACHÉ ET EN SÉCURITÉ, APPELEZ LES SECOURS

Où ? : Donnez votre position mais également celle de vos agresseurs.

Quoi ? : Nature de l'attaque (explosion, fusillade, attaque à l'arme blanche...)

Qui ? : Nombre d'assaillants, description physique et attitude, estimation du nombre de personnes blessées ou cachées.

- Comment se comportent-ils ?
- Regardent-ils la télé ?
- Quels moyens de communications ont-ils ?
- Ne raccrochez pas !

4. RÉSISTER

SI SE CACHER OU ÉVACUER EST IMPOSSIBLE, ET SI VOTRE VIE EST EN DANGER

- Tentez de neutraliser le terroriste à plusieurs.
- Distrayez l'adversaire (criez)
- Protégez-vous avec un bouclier de fortune (sac, vêtement enroulé autour de l'avant-bras).

VIGIPIRATE

FAIRE FACE ENSEMBLE

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.

6.1.2 Cas particuliers

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 (tabouret, chaise, etc.).
- 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.

En cas d'explosion et 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.

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

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.

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 du 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.

6.2 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 d'attaque. 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 ;
- limitez l'intoxication en vous déshabillant 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 ;
- contactez au plus vite les services de secours et de soins en appelant le : 15, 18, 112 ou 114 ;
- 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 ;
- 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.

PREMIER MINISTRE

Liberté
Égalité
Fraternité

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 :

MASQUE ;
MOUCHOIR ;
FOULARD ;
TISSUS HUMIDES

2 SI VOUS VOUS SENTEZ MAL, NE VOUS ALLONGEZ PAS, NE VOUS ASSEYEZ PAS

Vous pourriez ne plus vous relever.

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, suivez les comptes :

- @Interieur_Gouv
- @gouvernementFR

Restez à l'écoute des consignes des autorités publiques.

3 QUITTEZ RAPIDEMENT LES LIEUX SEMBLANT PRÉSENTER UN DANGER

En cas d'odeur anormale ou 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 VOTRE PREMIÈRE COUCHE DE VÊTEMENTS

Essayez de ne pas 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

Précisez votre emplacement et s'il faut intervenir rapidement sur un cas grave.

18/112 POMPIERS — 15 SAMU

114
NUMÉRO D'URGENCE POUR LES PERSONNES SOURDES ET MALENTENDANTES

7 NE RENTREZ SURTOUT PAS CHEZ VOUS, NE VOUS RENDEZ PAS À L'HÔPITAL

Attendez impérativement les secours et suivez leurs consignes, vous risqueriez de contaminer vos proches !

8 REJOIGNEZ UN POINT DE REGROUPEMENT ORGANISÉ PAR LES SECOURS, OÙ DES SOINS VOUS SERONT DONNÉS

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

Secrétariat général de la défense et de la sécurité nationale

7 GÉRER L'APRÈS-ATTENTAT

7.1 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.

7.2 Vous avez été victime d'une attaque terroriste

À la suite d'un acte terroriste, dès les premières heures, les victimes sont prises en charge par les services d'urgence. La phase d'urgence passée, les victimes peuvent déposer plainte et bénéficier d'un accompagnement et de droits spécifiques.

7.2.1 La prise en charge en urgence

Sur les lieux de l'acte terroriste ou à proximité, il est important de vous signaler aux forces de police et de gendarmerie ou aux services de secours. Des cellules d'urgence médico-psychologique (CUMP) 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, le Premier ministre peut activer la cellule interministérielle d'information du public et d'aide aux victimes - *InfoPublic*. Elle est chargée d'informer le public et d'accompagner les victimes et leurs proches, par téléphone. Un centre d'accueil des familles et différents lieux de prise en charge médico-psychologique pourront être mis en place.

Les recommandations et informations de la cellule *InfoPublic* peuvent être suivies à la radio, à la télévision et sur les réseaux sociaux officiels (Twitter et Facebook : @gouvernementFR, @Interieur_gouv).

7.2.2 L'accompagnement des victimes de terrorisme

▶ Contacter le numéro d'aides aux victimes 116 006

Le numéro européen 116 006[8], opéré par la fédération France Victimes, permet d'être orienté vers l'association ou le service susceptible d'apporter une réponse appropriée à chaque situation. Des professionnels informent les victimes sur leurs droits et les démarches à effectuer.

Ce service est gratuit, anonyme, ouvert à tous et disponible tous les jours de l'année de 9 heures à 20 heures.

▶ Les associations d'aide aux victimes

Sur l'ensemble du territoire national, des associations d'aide aux victimes offrent une prise en charge gratuite, personnalisée et confidentielle à toutes les victimes d'infractions pénales, dont les victimes du terrorisme. Des professionnels (juristes, psychologues, intervenants sociaux) informent les victimes sur leurs droits, apportent leur écoute, et les accompagnent dans leurs différentes démarches.

[8] *Ou+33 1 80 52 33 76 hors Hexagone.*

Trouver l'association d'aide aux victimes la plus proche de son domicile : https://www.justice.gouv.fr/annuaire/lieux-daccueil-daide-aux-victimes/associations-daide-aux-victimes

La cellule d'aide médico-psychologique (CUMP)

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.

7.2.3 Les droits spécifiques des victimes du terrorisme

Afin de bénéficier de ces droits spécifiques, il faut au préalable être reconnu officiellement victime du terrorisme par les autorités compétentes :

- par l'autorité judiciaire ;
- et/ou par le Fonds de garantie des victimes d'actes de terrorisme et d'autres infractions (FGTI).

Les victimes du terrorisme peuvent bénéficier des droits spécifiques suivants :

- indemnisation par le FGTI ;
- prise en charge des frais de santé causés par l'attentat ;
- bénéfice de mesures prévues pour les victimes civiles de guerre ;
- reconnaissances honorifiques spécifiques (dont la médaille nationale de reconnaissance aux victimes du terrorisme) ;
- conseils et assistance sur le plan fiscal.

Pour plus d'informations, rendez-vous sur le site : https://www.info.gouv.fr/guide-victimes

Pour plus d'information sur le plan fiscal rendez-vous sur le site : https://www.impots.gouv.fr/actualite/accompagnement-des-victimes-et-des-familles-de-victimes-dacte-de-terrorisme

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 PIRATE MOBTER permet d'intervenir en cas d'attaque dans les transports collectifs terrestres.

Le délégué interministériel à l'aide aux victimes (DIAV)

Le décret 2017-1240 du 7 août 2017 a institué un délégué interministériel à l'aide aux victimes placé auprès du Garde des Sceaux, ministre de la Justice.

Le *délégué interministériel à l'aide aux victimes* (DIAV) coordonne l'action des différents ministères en matière de suivi et d'accompagnement des victimes d'actes de terrorisme, d'accidents collectifs, de catastrophes naturelles, de sinistres sériels et d'autres infractions pénales. Il veille à l'efficacité et à l'amélioration des dispositifs d'aide aux victimes et coordonne l'ensemble des actions des ministères dans leurs relations avec les associations de victimes et d'aide aux victimes. Le DIAV prépare les réunions du comité interministériel de l'aide aux victimes et assure le pilotage, le suivi, la coordination et le soutien des comités locaux d'aide aux victimes. Enfin, il coordonne, en tant que de besoin, les services de l'État pour l'organisation des hommages et des commémorations.

Documentation

Documentation générale

Livre blanc sur la défense et la sécurité nationale de 2013, disponible en ligne sur :
http://www.livreblancdefenseetsecurite.gouv.fr/

Revue nationale stratégique de 2025, disponible en ligne sur :
https://www.sgdsn.gouv.fr/publications/revue-nationale-strategique-2025

Plan d'action contre le terrorisme du 13 juillet 2018, disponible en ligne sur :
https://www.sgdsn.gouv.fr/files/files/Publications/plan-d-action-contre-le-terrorisme-v8.pdf

Arrêté du 3 décembre 2020 relatif à la définition des scénarios standard nationaux et fixant les conditions applicables aux missions d'aéronefs civils sans équipage à bord exclues du champ d'application du règlement (UE) 2018/1139

Arrêté du 3 décembre 2020 relatif à l'utilisation de l'espace aérien par les aéronefs sans équipage à bord

Prévention de la radicalisation

Plan national de prévention de la radicalisation du 23 février 2018, disponible en ligne sur : https://www.cipdr.gouv.fr/pnpr/

Guide interministériel de prévention de la radicalisation, mars 2016, disponible sur : https://www.cipdr.gouv.fr/ressources-pratiques/

Guide des bonnes pratiques en matière de contre-discours, octobre 2021, disponible sur : https://www.cipdr.gouv.fr/ressources-pratiques/

Sites internet

https://www.info.gouv.fr/risques

https://www.sgdsn.gouv.fr/vigipirate/les-fiches-de-recommandations-et-de-bonnes-pratiques

https://www.info.gouv.fr/risques/reagir-en-cas-dattaque-terroriste

https://www.fondsdegarantie.fr/acte-terrorisme-france/

https://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/

https://fildariane.diplomatie.gouv.fr/fildariane-internet/accueil W

Prévention de la radicalisation

https://www.cipdr.gouv.fr/prevenir-la-radicalisation/

https://www.dgsi.interieur.gouv.fr/nous-contacter-radicalisation

Guides de bonnes pratiques

L'ensemble des guides de bonnes pratiques VIGIPIRATE sont consultables sur le site Internet suivant : https://www.sgdsn.gouv.fr/vigipirate

Formation en ligne

Une formation en ligne (MOOC), ouverte à tous, est disponible sur le site Internet suivant : https://vigipirate.gouv.fr/

FR-Alert

Toutes les informations sur le dispositif d'alerte et d'information des population FR-Alert est disponible sur le site internet suivant : https://fr-alert.gouv.fr/

GLOSSAIRE

CNRLT Coordination national du renseignement et de la lutte contre le terrorisme, placé auprès du Président de la République, il coordonne l'action des services de renseignement et s'assure de leur bonne coopération.

FR-Alert FR-Alert est le nouveau dispositif d'alerte et d'information des populations. Déployé sur le territoire national depuis fin juin 2022, FR-Alert permet de prévenir en temps réel toute personne détentrice d'un téléphone portable de sa présence dans une zone de danger afin de l'informer des comportements à adopter pour se protéger.

ISPS Code international pour la sûreté des navires et des installations portuaires (en anglais : *International Ship and Port Facility Security Code*)

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.

ODS Objectifs 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 Le système d'alerte et d'informations aux populations (SAIP) est un ensemble d'outils qui permet d'avertir la population d'une zone donnée, d'un danger imminent et de l'informer sur la nature du risque et le comportement à tenir. Basé sur la multidiffusion des messages, il rassemble donc différents vecteurs ainsi qu'un logiciel de déclenchement permettant aux maires et aux préfets d'assurer la protection de leur population.

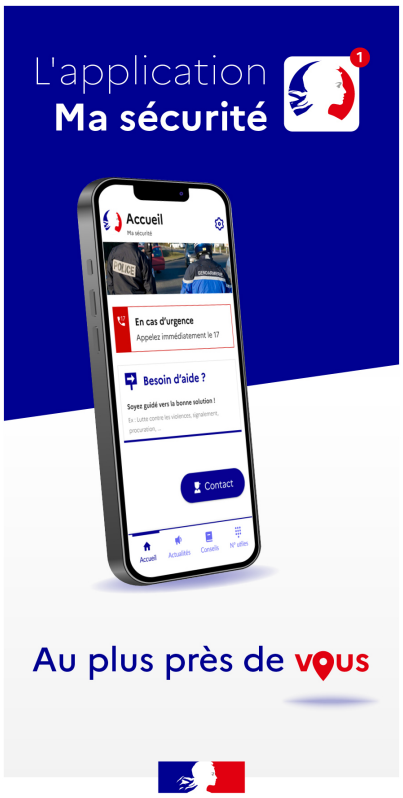
SAIV Sécurité des activités d'importance vitale. Dispositif de sécurité qui donne un cadre juridique spécifique aux opérateurs d'importance vitale (OIV) pour les faire coopérer à la protection de leurs installations critiques contre toute menace, notamment à caractère terroriste.

SIG Service d'information du gouvernement, service du Premier ministre, placé 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.

APPLICATION UTILE



Destinée à tout citoyen, l'application « **Ma Sécurité** » est une application officielle du ministère de l'Intérieur, développée en partenariat avec la Police nationale et la Gendarmerie nationale, pour permettre aux citoyens de signaler en toute sécurité des situations d'urgence ou de risque, notamment en cas de handicap auditif ou de difficulté à parler.

En cas d'alerte reçue via l'application, les services d'urgence sont notifiés en temps réel avec la localisation exacte — ce qui accélère l'intervention.

▶ Envoi de SMS d'urgence
Permet d'alerter les services d'urgence (17, 18, 15) par SMS automatique avec géolocalisation précise.

▶ Alerte silencieuse
En cas de danger (violence, intrusion, harcèlement), l'utilisateur peut déclencher une alerte sans parler, sans risque d'être entendu.

▶ Partage de localisation en temps réel
Permet de partager sa position avec un proche de confiance ou les services d'urgence.

▶ Accès aux numéros d'urgence
Accès rapide aux numéros 17, 18, 15, 114, 116 006, 0 800 005 696, etc.

▶ Fonctionnalité TPH
Conçue pour les personnes sourdes ou malentendantes, en complément du numéro 114.

https://www.interieur.gouv.fr/Ma-Securite

NUMÉROS UTILES

En cas d'attaque ou pour signaler une situation anormale

17	Police nationale / Gendarmerie nationale
112	Numéro d'urgence européen
114	Numéro d'urgence dédié aux personnes sourdes et malentendantes et permet d'envoyer un SMS d'urgence aux services de secours (15, 17 ou 18).

En cas d'attaque avec un produit toxique ou en présence d'une urgence vitale

15	SAMU (urgences médicales)
18	Sapeurs-pompiers (Urgences liées aux incendies, accidents, secours en milieu naturel ou urbain, assistance aux personnes en détresse)
112	Numéro d'urgence européen
114	Numéro d'urgence dédié aux personnes sourdes et malentendantes et permet d'envoyer un SMS d'urgence aux services de secours (15, 17 ou 18). (pour les personnes ayant des difficultés à entendre ou à parler).

Dans un train ou un transport collectif

Plateforme de signalement par appel au 31 17 ou par SMS au 31 177 OU application mobile « Ma sécurité », catégorie « Transports et mobilités ».

Victime d'un acte terroriste

15 — SAMU (urgences médicales)

Effectuer un signalement

0 800 005 696 (numéro vert) — Police nationale / Gendarmerie nationale

116 006 — Numéro national d'aide aux enfants en danger

3919 — Numéro national d'écoute et d'orientation pour les victimes de violences physiques, psychologiques, sexuelles, économiques ou conjugales

NOTES

PREMIER
MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général
de la défense
et de la sécurité nationale

51, boulevard de La Tour-Maubourg - 75007 Paris
N 48°51'23,5" E 2°18'43,2"
www.sgdsn.gouv.fr