

Paris, le 1^{er} décembre 2016



Note de posture VIGIPIRATE

LE HAUT
FONCTIONNAIRE
DE DÉFENSE ET DE
SÉCURITÉ

n° 2016/07

Objet : Adaptation de la posture VIGIPIRATE « Transition 2016-2017 »

Réf. : Partie publique du Plan gouvernemental de vigilance, de prévention et de protection face aux menaces d'actions terroristes n°10200/SGDSN/PSN/PSE du 1^{er} décembre 2016

PJ :
- annexe n°1 : Tableau des mesures de vigilance, de surveillance et de contrôle
- annexe n°2 : Recommandations pour la sécurisation des lieux de rassemblement ouverts au public
- annexe n°3 : Le rôle des citoyens en matière de vigilance

La posture VIGIPIRATE « Transition 2016-2017 » **s'applique à partir du 1^{er} décembre 2016** et prend en considération les vulnérabilités propres aux périodes de la fin d'année 2016 et du premier trimestre 2017. Elle s'applique, sauf événements particuliers, **jusqu'au 20 mars 2017**, date de la publication de la liste officielle des candidats à l'élection présidentielle.

A la suite des derniers attentats qui ont frappé la France et des dispositions législatives adoptées en 2016, le Premier ministre a décidé d'adapter le plan VIGIPIRATE à la persistance d'un haut niveau de la menace terroriste.

Un nouveau plan VIGIPIRATE 2016, approuvé en Conseil de défense et de sécurité nationale du 30 novembre 2016, entre en vigueur pour la présente posture. Il reprend l'architecture et les principes de fonctionnement de l'édition 2014 mais s'articule autour de 3 niveaux :

- un niveau dit de « *vigilance* », qui correspond à la posture permanente de sécurité ;
- un niveau « *sécurité renforcée-risque attentat* », qui adapte la réponse de l'État à une menace terroriste élevée, voire très élevée. Ce niveau peut s'appliquer à l'ensemble du territoire national ;
- un niveau « *urgence attentat* », qui serait instauré immédiatement après un attentat ou en cas d'entrée en action d'un groupe terroriste identifié mais non encore localisé.

En application du nouveau plan VIGIPIRATE, **l'ensemble du territoire national est élevé au niveau « sécurité renforcée - risque attentat »**.
Le plan Vigipirate public 2016 « Faire face ensemble » et les logos des trois nouveaux niveaux sont téléchargeables sur l'espace <http://www.gouvernement.fr/vigipirate>

L'effort est réorienté vers les sites liés aux manifestations festives, religieuses, touristiques et politiques de fin d'année 2016 et du 1^{er} trimestre 2017.

La posture met l'accent sur :

- le renforcement de la sécurité des grands espaces de commerce et des lieux de culte marqués par une forte affluence pendant les fêtes de fin d'année et la période des soldes d'hiver ;
- le maintien d'une **vigilance renforcée dans les établissements d'enseignement** et dans les établissements de santé, médico-sociaux et sociaux. Concernant les **établissements d'enseignement supérieur et de recherche, un guide des bonnes pratiques réalisé conjointement par le SGDSN et le ministère chargé de l'enseignement supérieur est disponible sur le site <http://www.encasdattaque.gouv.fr>**
- le maintien de la sécurité dans le domaine des transports, en particulier lors des départs et retours des vacances scolaires ;
- le renforcement de la vigilance **dans les sites touristiques majeurs** et lors des événements et des rassemblements politiques précédant l'ouverture officielle de la campagne présidentielle. **La vigilance est renforcée à proximité et dans les espaces de loisirs (cirques, salles de spectacle et parcs de loisirs).**

Pour la pleine efficacité des mesures arrêtées, cette posture doit être l'occasion donnée à l'ensemble des responsables de sa mise en œuvre d'effectuer une revue des dispositifs de sécurité existants et de sensibiliser l'ensemble des acteurs de terrain aux spécificités de la période abordée.

L'ensemble des actions de vigilance, de surveillance et de contrôle est récapitulé en annexe n°1.

Ces consignes doivent être retransmises aux acteurs du champ culturel conformément à la chaîne d'information et d'alerte du MCC (cf note du directeur de cabinet du 23 décembre 2015), notamment, pour les DRAC, les acteurs considérés comme sensibles (cf. votre cartographie régionale), afin qu'ils organisent leur propre protection, et d'en rendre compte au préfet de chaque département.

Tout établissement recevant du public est invité à définir des procédures simples d'alerte et de réaction en cas d'attaque terroriste auxquelles ses agents doivent être sensibilisés, en s'inspirant des guides de bonnes pratiques VIGIPIRATE réalisés.

Trois guides de bonnes pratiques sont à votre disposition sur le site du ministère :

<http://www.culturecommunication.gouv.fr/Actions-de-renforcement-et-de-surveillance-des-lieux-culturels>

- guide à destination des organisateurs de rassemblements et festivals culturels
- guide à destination des dirigeants de salles de spectacle, de cinémas ou de cirques
- guide à destination des dirigeants d'établissements culturels patrimoniaux (musées, monuments historiques, archives et bibliothèques)

Ces guides sont également disponibles sur le site du gouvernement <http://www.encasdattaque.gouv.fr> , ainsi que le « guide à destination des présidents d'université, des directeurs d'établissements d'enseignement supérieur et des référents défense et sécurité ».

Ces guides ont vocation à être diffusés le plus largement possible.

Par ailleurs, vous trouverez ci-joint une fiche de « recommandations pour la sécurisation des lieux de rassemblement ouverts au public » (annexe 2) et une fiche relative au rôle des citoyens en matière de vigilance » (annexe 3).

Enfin, il convient de rappeler à vos collaborateurs appelés à effectuer des missions à l'étranger de consulter préalablement le site du ministère des affaires étrangères <http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/> afin de prendre connaissance des consignes de sécurité spécifiques au pays concerné et à s'inscrire sur le site *Ariane* du ministère des affaires étrangères et du développement international.

Le Haut fonctionnaire de défense et de sécurité

Marc Oberlis

Signé : Marc Oberlis

Posture « Transition 2016-2017 »**TABLEAU DES MESURES DE VIGILANCE, DE SURVEILLANCE ET DE CONTRÔLE**

Nota : les mesures nouvelles figurent en gras dans le tableau

| N° mesure | Mesure | Commentaires |
|-------------------------------------|---|---|
| ALR 11-01 | Activer les cellules de veille et d'alerte et les cellules de crise | Les cellules de crise des ministères sont activées en tant que de besoin. |
| ALR 11-02 | Diffuser l'alerte au grand public | <p>- affichage du nouveau logo « Sécurité renforcée - risque attentat » à l'entrée des sites accueillant du public :</p> <div style="text-align: center;">  </div> <p>- diffusion de messages d'appel à la vigilance dans les établissements recevant du public (ERP), y compris en langues étrangères ;</p> <p>- information claire des visiteurs et spectateurs à l'entrée et sur les sites web de chaque établissement concernant les mesures de contrôle en vigueur : utiliser les pictogrammes en ligne sur le site http://www.culturecommunication.gouv.fr/Actions-de-renforcement-et-de-surveillance-des-lieux-culturels</p> <p>- utilisation de l'application smartphone SAIP d'alerte aux populations, principalement conçue pour diffuser les alertes sur des attentats.</p> |
| RSB 11-01 RSB 12-01 RSB 13-01 | Renforcer la surveillance et le contrôle | <p>L'effort de vigilance porte notamment sur les rassemblements liés aux fêtes de fin d'année (cf annexe 2). La sensibilisation à la détection et au signalement de comportements suspects doit être réalisée (cf annexe 3).</p> <p><u>MANIFESTATIONS EN EXTÉRIEUR</u></p> <p>1) dans une enceinte close d'un établissement :</p> <p>- contrôle visuel <u> systématique </u> des visiteurs en demandant à ceux ayant des vêtements amples, susceptibles de dissimuler une arme automatique, de les</p> |

| | | |
|-------------------------------------|--|--|
| | | <p>ouvrir, ainsi que du contenu de leurs sacs ;</p> <p>- interdiction des valises et des sacs de grande contenance.</p> <p><u>Toute personne refusant le contrôle doit se voir interdire l'entrée de l'établissement.</u></p> <p><i>2) sur la voie publique :</i></p> <p>Ces manifestations sont soumises à des restrictions qui peuvent être plus importantes selon les directives préfectorales.</p> <p>Ces dispositions ne font pas obstacle à la liberté de l'organisateur de renoncer à la tenue d'une manifestation dès lors qu'il le juge nécessaire, soit parce qu'il estime ne pas être en mesure de satisfaire pleinement à ses obligations de sécurité du public, soit en fonction de circonstances spécifiques liées notamment à la thématique de la manifestation. Un contact avec les services de police locaux est indispensable afin d'aider les organisateurs dans leur appréciation du risque.</p> |
| BAT 11-02 BAT 12-02 BAT 13-02 | Restreindre voire interdire le stationnement et/ou la circulation aux abords des installations et bâtiments désignés | <p>A l'appréciation des préfets pour le ciblage.</p> <p>En accord avec les forces de police, des mesures de sécurité passive (barriérage, plots béton, chicane...), voire la restriction ou l'interdiction de circulation peuvent utilement être déployées.</p> |
| BAT 11-03 BAT 12-03 | Renforcer la surveillance aux abords des installations et bâtiments désignés | Renforcement de la vigilance externe par l'installation de dispositifs de vidéoprotection, prioritairement pour les ERP et les établissements d'enseignement supérieur. |
| BAT 21-01 BAT 22-01 BAT 23-01 | Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier) | <p>1) CONTRÔLE DES VISITEURS / SPECTATEURS :</p> <p>- pour les établissements équipés de portiques : passage <u>systematique</u> sous portique ;</p> <p>- pour les établissements équipés de magnétomètres : utilisation <u>systematique</u>.</p> <p>- valises et sacs de grande contenance : interdits dans les ERP non équipés de scanner à rayons X.</p> <p>Pour les établissements concernés, il convient d'informer le public (site web et affichage) de cette mesure, et de modifier le règlement intérieur de l'établissement.</p> <p><u>Toute personne refusant l'un de ces contrôles doit se voir interdire l'entrée de l'établissement.</u></p> <p>Toutefois, pour les chefs d'établissement de l'enseignement supérieur du secteur de la culture qui reçoivent des étudiants, ces derniers peuvent, selon la situation de leur établissement, autoriser leurs professeurs et leurs étudiants à introduire des valises, des sacs et des étuis d'instruments de musique après contrôle visuel du contenu.</p> |

| | | |
|-----------|---|--|
| | | <p>2) POUR LE PERSONNEL :</p> <p>Badge (ou pièce d'identité) obligatoire pour l'accès à l'établissement. A l'appréciation des chefs d'établissement et selon la situation de leur établissement, ceux-ci peuvent procéder au renforcement des contrôles (inspection visuelle des sacs) pour les personnels des manifestations extérieures, les prestataires extérieurs, les personnels intérimaires et temporaires, et en tant que de besoin selon la taille, la configuration, le site ou le caractère symbolique de l'établissement, pour les personnels permanents, après information/consultation du CHSCT spécial d'établissement consacré aux mesures de sûreté et de sécurité.</p> <p>3) LIMITATION DES ACCÈS AUX SITES :</p> <ul style="list-style-type: none"> - accès visiteurs : limitation du nombre d'accès à l'initiative des chefs d'établissement ; - autres accès : les accès réservés à du personnel spécifique (artistes, prestataires extérieurs, agents de l'établissement) doivent faire l'objet d'un renforcement des contrôles tel qu'indiqué ci-dessus. <p>4) VÉHICULES ENTRANTS :</p> <p>contrôle <u>systématique</u> et vérification de la marchandise.</p> |
| BAT 31-01 | Renforcer la surveillance interne et limiter les flux (dont interdiction de zone) | Limitation des flux de visiteurs si l'affluence est jugée trop importante. |
| CYBER | Protéger logiquement ses systèmes d'information | <p>1) CONSEILS AUX UTILISATEURS</p> <ul style="list-style-type: none"> - demeurer vigilant sur les courriels reçus et, en cas de doute, ne pas ouvrir les pièces jointes ni cliquer sur les liens internet y figurant ; - limiter les navigations vers des sites internet n'ayant pas de rapport avec l'activité professionnelle ; - rendre compte aux responsables locaux de la sécurité des systèmes d'information de tout comportement anormal du poste de travail. <p>2) CONSEILS AUX RESPONSABLES ORGANIQUES</p> <ul style="list-style-type: none"> - assurer une revue des droits des comptes les plus privilégiés et en assurer une supervision ; - contrôler l'application de la politique des mots de passe et renouveler les mots de passe des comptes les plus privilégiés ; - vérifier ou mettre en place les mesures de prévention en matière de déni de service. <p><i>Vous pouvez consulter les notes d'information et les guides de l'ANSSI sur le site www.ssi.gouv.fr/administration/bonnes-pratiques/ concernant notamment :</i></p> <ul style="list-style-type: none"> - <i>guide d'hygiène</i> - <i>guide de bonnes pratiques</i> |

| | | |
|--|--|--|
| | | <ul style="list-style-type: none">- <i>dénis de service (prévention et réaction)</i>- <i>sécurisation des sites web</i>- <i>comprendre et anticiper les attaques en DDoS</i>- <i>défigurations de sites</i>- <i>cyberattaques (prévention, réaction)</i>- <i>conduite à tenir en cas d'intrusion</i>- <i>mesures de prévention relatives à la messagerie</i>- <i>politique de restrictions logicielles sous Windows</i> |
|--|--|--|

RECOMMANDATIONS POUR LA SÉCURISATION DES LIEUX DE RASSEMBLEMENT OUVERTS AU PUBLIC

Cette fiche concerne la protection des lieux de rassemblement ouverts au public et a pour objectif de rappeler les recommandations nécessaires à la sécurité de tels événements.

Il est primordial que les organisateurs de rassemblements se coordonnent avec les forces de police, de gendarmerie, de police municipale et de sapeurs-pompiers préalablement à la tenue de tels événements.

Cette fiche doit être largement diffusée.

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 et des échanges avec les forces de sécurité intérieure.

1 – IDENTIFIER LES MENACES ET LES VULNÉRABILITÉS

Il faut d'abord évaluer la sensibilité du rassemblement en lien avec les autorités de police administrative (préfet et maire) :

- 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 ?

Les différentes attaques possibles doivent être envisagées :

- jet ou dépôt d'un engin explosif ;
- véhicule piégé en stationnement aux abords du site ;
- véhicule bélier ;
- fusillade ;
- attaque à l'arme blanche.

Il convient de choisir le lieu d'implantation de l'événement qui présentera le moins de vulnérabilités. Il est ainsi préférable d'éviter de s'installer au-dessus d'un parking ou en contrebas de voies de circulation.

2 – ORGANISER LA SÉCURITÉ DE L'ÉVÉNEMENT

Il est primordial que les organisateurs de rassemblements se coordonnent avec les forces de sécurité intérieure et les sapeurs-pompiers. Les mesures ci-dessous sont données à titre d'exemple et doivent être adaptées en fonction de la situation.

2-1 Au niveau de la périphérie

- en lien avec les forces de l'ordre, interdire le stationnement de tout véhicule aux abords immédiats du lieu de 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, 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 ;
- mettre en place un système de vidéo-protection donnant, en priorité, sur les accès au site.

2-2 Au niveau de 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 sortants ;
- aménager, au niveau des accès, des points de contrôle armés 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 visant à entraver toute intrusion de véhicule-bélier (blocs de béton, véhicule, etc.) ;
- contrôler par une présence humaine les points de sorties 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.

2-3 Au niveau des volumes intérieurs

- désigner un responsable sûreté qui sera l'interlocuteur unique des forces de l'ordre 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 24h/24 par au moins un opérateur qui visualisera les images du système de vidéo-protection mis en place ;
- sensibiliser la totalité des exposants à la remontée de tout signalement d'actions de repérage et à la réaction à avoir en cas d'attaque ;
- installer des écrans et des haut-parleurs pouvant diffuser une alerte (pré-enregistrée si possible) ;
- organiser et contrôler les livraisons.

LE RÔLE DES CITOYENS EN MATIÈRE DE VIGILANCE

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.

1 – POURQUOI SIGNALER UN COMPORTEMENT SUSPECT ?

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'organisation d'un attentat requiert le plus souvent une préparation et des moyens humains et matériels. La plupart des attaques terroristes font d'abord l'objet d'un repérage pour identifier les mesures de sécurité mises en place afin de les contourner, les chemins d'accès, etc.

A l'occasion des différentes phases de l'élaboration d'une telle opération, les terroristes sont contraints, à un moment ou à un autre, de s'exposer.

2 – COMMENT DÉTECTER UNE SITUATION SUSPECTE ?

La préparation d'une action terroriste n'a pas toujours la perfection qu'on imagine. Des incohérences apparaissent et vous pouvez les détecter. Faites appel à votre bon sens et à votre intuition. Vous devez savoir vous étonner de ces incohérences et vous demander si cela ne mérite pas un signalement. Il faut par conséquent apprendre à être un observateur de son environnement (voisinage, vie professionnelle, transports en commun, etc.).

3 – COMMENT SE PRÉPARE UNE ACTION TERRORISTE ?

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

3-1 Le choix des cibles

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

3-2 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 :

- a) 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.) ;
- b) rassemblement d'un maximum d'informations sur la cible :
 - recherche de complicités internes ;
 - demandes de renseignements sur les mesures de sécurité par le biais de discussions en apparence anodines ;
 - observation de la manière dont se déroulent les contrôles de sécurité, voire test de ces mêmes contrôles via de fausses alertes (type alerte à la bombe) ;
 - prises de vues (photographie ou film) des infrastructures du site ciblé et du dispositif de protection mis en place (porte d'entrée d'un ministère, patrouille de militaires, etc.) ;
 - prises de notes sur les dispositifs de sécurité (plan du site, positionnement des caméras de surveillance, des portes d'entrée et de sortie, etc.) ;
 - recherches d'informations par internet (réseaux sociaux, plans de vues aériennes, etc.) ;
 - utilisation de techniques de dissimulation ou de camouflage.

3-3 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 :

- un colis ou un sac abandonné. Un sac positionné dans un lieu de passage important doit entraîner un signalement ;
- un véhicule en stationnement prolongé à proximité d'un lieu de rassemblement (marché, lieu de culte, etc.) ou d'un site sensible (mairie, ambassade, etc.).

Comment signaler et réagir ?

Si vous êtes témoin d'un comportement suspect, restez discret. 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.).

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