VIGIPIRATE

ORGANISER UN CONFINEMENT FACE À UNE MENACE TERRORISTE

Fiche pratique à destination des responsables d'établissement accueillant du public.

Pour garantir au mieux la sécurité des personnes, les établissements accueillant du public devront mener une réflexion sur la question du confinement, de la décision à la levée de celle-ci.

Cette fiche pratique à destination des responsables de sécurité et de sûreté de ces établissements dispense des recommandations et des bonnes pratiques à adopter pour se préparer face à la menace terroriste.

En cas d'attaque armée, il est nécessaire de déterminer la réponse la plus appropriée à la situation. Celle-ci n'est pas figée, elle évolue : adoptez vos modes de réaction aux circonstances.

Le confinement est envisageable **si l'attaque est extérieure** au site dans lequel vous vous trouvez ou **si l'attaque survient à l'intérieur** mais que s'échapper semble trop dangereux.

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

1 Comment se préparer ?

Pour limiter les risques et les dangers que peut entraîner le confinement, certaines recommandations, tirées de plusieurs confinement réels en 2017, permettent de se préparer et d'anticiper les situations d'urgence :

- **Elaborer un plan de mise en sûreté** prévoyant :
  - les missions des personnels ;
  - les zones possibles de confinement ;
  - les coordonnées des forces de sécurité intérieure les plus proches ;
  - Les missions de chacun suivant les périodes de l'année (jours fériés, horaires atypiques, vacances scolaires, etc.) ;
  - la reprise de l'activité normale.
- **S'appuyer sur un poste central de sûreté ou un moyen de centraliser l'information,** suivant la taille de l'établissement et désigner un responsable.
- **Identifier les personnels de confiance** qui peuvent seconder le responsable de l'établissement pour accueillir, sécuriser et rassurer le public présent sur le site.
- **Informer et sensibiliser** les personnels plusieurs fois dans l'année.
- **Organiser des exercices,** à différentes périodes de l'année au sein de l'établissement (week-end, personnel réduit, etc.) afin d'identifier les vulnérabilités.
- **Identifier plusieurs zones de confinement,** mécaniquement sanctuarisables, si possible avec un point d'eau et des toilettes et dont l'accès est exclusivement réservé aux acteurs gestionnaires du risque.
- **Envisager les difficultés potentielles de communication** avec le public et s'y préparer (langage corporel, etc.).

L'organisation de la coordination est fondamentale

- **Etablir et conserver un contact permanent** entre un responsable identifié au sein du site et les forces de sécurité intérieure.
- **Mettre en place des moyens de communication interne** entre les différentes zones de l'établissement (radios, logiciels internes, etc.).
- **Rendre accessibles les moyens de transmission aux forces de sécurité intérieure** (moyens radios mobiles supplémentaires, report de vidéoprotection, etc.).
- **Préenregistrer un message d'alerte le moins anxiogène possible.**

2 Comment organiser un confinement ?

2.1 - Décider du confinement

a) Qui décide ?

La décision de confinement relève du bon sens. Elle est prise le plus souvent par le responsable de l'établissement mais peut également l'être par l'ensemble des personnels directement au contact d'une situation l'exigeant. Elle peut être prise par l'ensemble des personnels.

Les personnels doivent être sensibilisés aux procédures prévues dans leur établissement.

b) Comment le mettre en place ?

Diffuser un message à l'attention du public en utilisant un ton non-anxiogène. L'objectif est d'éviter à tout prix de déclencher une panique. Il est conseillé de préenregistrer un message.

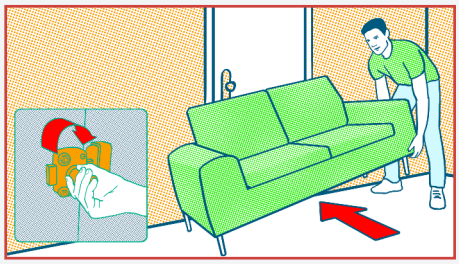
Envisager l'installation d'un système de sonorisation dans tout ou partie de l'établissement.

Prévoir un système d'appel automatique sur les postes fixes avec un message pré-enregistré et/ou envoi de SMS aux personnels.

2.2 - Gérer le confinement

Suivant le niveau de menace connu ou ressenti, il est possible de prendre certaines dispositions :

- bloquer les portes avec des moyens de fortune ;
- éteindre les lumières ;
- s'éloigner des portes et fenêtres ;
- s'allonger au sol ;
- faire respecter le silence (mode silence des téléphones).



Une fois à l'abri, prévenez les forces de sécurité en donnant les informations essentielles (où, quoi, qui, combien, comment).

Tenir informées du mieux possible les forces de sécurité intérieure sur les conditions du confinement.

Prévenez ou faites prévenir les sites voisins.

Travailler sur l'attitude rassurante des personnels. Oser répéter les informations et **communiquer régulièrement** avec le public. Informer sur un point d'eau ou des toilettes éventuelles dans la zone de confinement.

Recommander aux personnes de rassurer leur entourage par message, plutôt que par conversation téléphonique (risque de saturation), et d'éviter de diffuser sur les réseaux sociaux des informations en temps réel.

Rester vigilant sur les comportements anormaux (stress extrême, comportement agressif ou suspect).

2.3 - Lever le confinement

Attendre l'autorisation des forces de sécurité intérieure pour lever le confinement.

Maintenir un encadrement rigoureux de la foule pour assurer une dispersion fluide lors de son évacuation.

Guider le public dans la direction de l'évacuation en fonction des consignes données par les autorités.

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

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

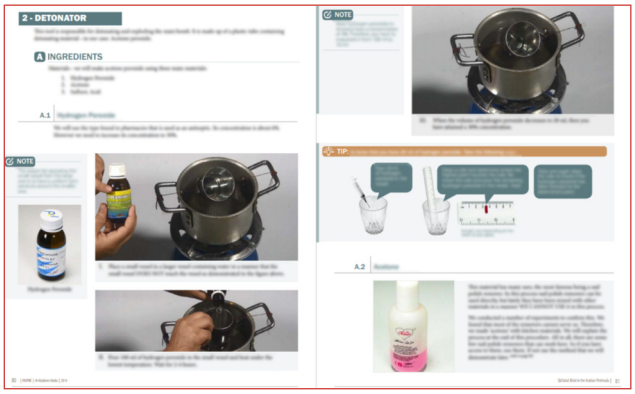
Maquette et impression : Pôle Conception graphique-Fabrication – DSAF/DPL – Juillet 2017.

PRODUITS CHIMIQUES :
SIGNALEMENT DE TOUT VOL OU UTILISATION SUSPECTE

Les derniers attentats ou actes de malveillance commis en Europe ont montré la capacité des criminels et terroristes à fabriquer des explosifs artisanaux ou des substances toxiques en utilisant des produits chimiques d'usage courant, souvent disponibles dans les magasins de bricolage, les jardineries, les grandes surfaces, etc.

Des tentatives d'attentats ont pu être déjouées grâce aux signalements de comportements ou d'achats suspects de produits chimiques (engrais, solutions de nettoyage de piscine, détachant, dissolvant, etc.).

- Novembre 2015 : **attentats de Paris** (stade de France, Bataclan) ;
- Mars 2016 : **attentats à l'aéroport de Bruxelles-Zaventen** et à la **station Maelbeek** (Belgique) ;
- Février 2017 : découverte d'un laboratoire de fabrication d'explosifs à **Montpellier** – attentat déjoué ;
- Avril 2017 : découverte d'un laboratoire de fabrication d'explosifs à **Marseille** – attentat déjoué ;
- Mai 2017 : **attentat de Manchester** (Royaume-Uni) ;
- Août 2017 : explosion d'un laboratoire de fabrication d'explosifs à **Alcanar** (Espagne) ;
- Eté 2017 : jets d'acide à **Londres** (Royaume-Uni) ;
- Août 2017: découverte d'un projet d'engin chimique à **Sidney** (Australie) ;
- Septembre 2017 : jet d'acide à **Marseille** ;
- Septembre 2017: découverte d'un **laboratoire clandestin** de fabrication d'explosifs à **Villejuif.**



Des recettes disponibles sur Internet

Un laboratoire de fabrication d'explosifs artisanaux

1 Comment détecter une utilisation suspecte de produits chimiques ?

En étant attentif à son environnement, chacun **peut détecter** la fabrication de substances permettant de commettre des attentats. Les éléments suivants, **constatés dans un lieu inapproprié, doivent vous alerter :**

- divers **produits chimiques** en quantité inhabituelle ;
- des **équipements** tels que des moyens de chauffage, des ustensiles de cuisine ou de la verrerie de laboratoire, des gants et lunettes de protection ;
- une **odeur** suspecte.

SUBSTANCES CHIMIQUES + MATÉRIELS INAPROPRIÉS (+ ODEURS) = SIGNALEMENT

2 Comment réagir et signaler ?

Si vous êtes témoin d'une utilisation suspecte de produits chimiques, **ne vous mettez pas en danger, restez discret et appelez sans délai les forces de sécurité intérieure** en composant le 17, 112 ou 114 (pour les personnes ayant des difficultés à entendre et à parler).

3 Quelles sont les obligations des professionnels qui commercialisent des produits chimiques ?

La réglementation française (*décret n°2017-1308 du 29 août 2017*) prévoit des mesures pour restreindre l'accès du grand public à des substances chimiques d'usage courant :

	Présence possible dans…	INTERDICTION de vendre aux particuliers (au delà d'une certaine concentration)	Autorisation de vendre aux particuliers avec obligation d'ENREGISTREMENT par le vendeur	SIGNALEMENT au point de contact national (PIXAF) de tout vol, perte, disparition ou transaction suspecte
Peroxyde d'hydrogène (7722-84-1)	Produits de blanchissage, décolorants capillaires, désinfectants, agents nettoyants	> 35% p/p	de 12 < % p/p ≤ 35	
Nitrométhane (75-52-5)	Carburants pour modèles réduits, solvants	> 40% p/p	de 30 < % p/p ≤ 40	
Acide nitrique (7697-37-2)	Décapants, traitement des métaux	> 10% p/p	de 3 < % p/p ≤ 10	
Chlorate de sodium (7775-09-9), **chlorate de potassium** (3811-04-9), **perchlorate de sodium** (7601-89-0) et **perchlorate de potassium** (77778-74-7)	Articles pyrotechniques	> 40% p/p		
Nitrate d'ammonium (6484-52-2)	Engrais, poche de froid			
Acétone (67-64-1)	Dissolvants, solvants			
Hexamine (100-97-0)	Additifs alimentaires, carburants solides pour réchauds de camping et pour moteurs à vapeur de modèles réduits			
Acide sulfurique (7664-93-9)	Déboucheurs de canalisation			
Nitrate de potassium (7757-79-1), **nitrate de sodium** (7631-99-4)	Engrais, conservateurs alimentaires			
Poudres d'aluminium (7429-90-5) et de **magnésium** (7439-95-4) **Nitrate de calcium** (10124-37-5) **Nitrate de magnésium hexahydraté** (13446-18-9)	Engrais			

Pour plus de détails, contacter le service central des armes (ministère de l'intérieur/SCA) :
sca-precurseurs-explosifs@interieur.gouv.fr

Quels critères permettent de détecter une transaction suspecte de produits chimiques à des fins malveillantes ?

Les critères suivants peuvent alerter un professionnel :

- absence d'explications cohérentes sur l'utilisation prévue des produits ;
- utilisation du produit inconnue de l'acheteur ;
- réticence à dévoiler l'utilisation du produit ;
- quantités, combinaisons ou concentrations inhabituelles de produits pour un usage domestique ;
- réticence de l'acheteur à donner les éléments nécessaires à l'enregistrement de la transaction ;
- paiement important en espèces ;
- tentative de communiquer le moins possible ;
- refus de tout produit de substitution ou de plus faible concentration.

Que faire en cas de vol, disparition ou transaction suspecte de produits chimiques réglementés ?

Les professionnels ont l'obligation de signaler tout vol, disparition ou transaction suspects au **point de contact national :**

Plateau d'Investigation eXplosifs et Armes à Feu de la Gendarmerie nationale
pixaf@gendarmerie.interieur.gouv.fr - 01 78 47 34 29 (24H/24H)

VOL ou DISPARITION ou TRANSACTION SUSPECTE = SIGNALEMENT

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

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

Maquette et impression : Pôle Conception graphique-Fabrication – DSAF/DPL – Octobre 2017.

RECOMMANDATIONS POUR LA SÉCURISATION DES LIEUX DE RASSEMBLEMENT OUVERTS AU PUBLIC

(Fiche actualisée en date du 2 novembre 2017)

Cette fiche traite de la protection des lieux de rassemblement ouverts au public (événements sportifs, festivals, marchés de Noël, braderies, etc.) et doit pouvoir servir de guide pratique aux organisateurs de ce genre de manifestations. Elle doit être largement diffusée. Certains des conseils délivrés ci-dessous peuvent ne pas être applicables à tous les sites. Ils doivent donc être adaptés en fonction de la configuration des lieux et du bon sens de circonstance.

1 Identifier les menaces et les vulnérabilités

Il faut d'abord évaluer la sensibilité du rassemblement en lien avec les autorités locales (préfet, maire, Police Nationale, Gendarmerie Nationale) :

- 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 à l'intérieur ou en périmétrie du site ;
- véhicule piégé en stationnement aux abords du site ;
- véhicule-bélier ;
- fusillade ou attaque suicide ;
- prise d'otage ;
- attaque à l'arme blanche.

2 Organiser la sécurité de l'événement

Il est primordial que les organisateurs de rassemblements se coordonnent avec le maire et le préfet, ainsi qu'avec les forces de police, de gendarmerie, les services de police municipale et d'incendie et de secours.

Par ailleurs, il peut être nécessaire de faire appel aux compétences de sociétés privées de sécurité pour renforcer la sécurité d'un tel événement.

2.1 - En périphérie du rassemblement

- **choisir le lieu d'implantation de l'événement qui présentera le moins de vulnérabilités.** Il est préférable de choisir le lieu du rassemblement de manière à limiter l'accès de véhicules (ne pas s'installer au débouché d'un axe important) ;
- **limiter ou interdire le stationnement** des véhicules 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 ;
- **cloisonner le flux des véhicules de l'espace de déambulation des piétons ;**
- **identifier le mobilier urbain** qui pourrait servir à dissimuler de l'explosif, le faire retirer par les autorités habilitées, 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. Des agents des sociétés privées de sécurité peuvent concourir à cette mission ;
- **identifier les points de vulnérabilité hauts** (immeubles surplombant) 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, en prenant en compte les dispositions du Code de la sécurité intérieure.

2.2 - Sur la périmétrie du rassemblement

- **aménager des points de contrôle ou de filtrage en nombre suffisant** aux entrées du site afin de fluidifier l'entrée du public. Leur efficacité repose sur la présence d'un superviseur, de moyens de communication et de procédures claires afin de diffuser l'alerte et de faciliter l'intervention des forces de sécurité intérieure en cas d'incident ;
- **maintenir le niveau de vigilance tout au long de l'événement mais également lors du moment sensible de sa dispersion** (le 22 mai 2017 à Manchester, au Royaume-Uni, un homme a fait détoner une charge explosive qu'il portait sur lui à la sortie de la salle de spectacle *Manchester Arena*), en rappelant régulièrement des messages de sensibilisation à destination du public (*via* la sonorisation de l'événement par exemple – « TOUS acteurs de la sécurité) » ;
- **installer une délimitation physique du périmètre extérieur** de l'événement au moyen de barrières reliées entre elles, de blocs en béton, de véhicules du comité d'organisation comme élément de barrage, etc. ;
- organiser un ou plusieurs cheminements jusqu'au point de contrôle en installant des barrières. Séparer, dans la mesure du possible, les flux entrants et les flux sortants ;
- **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 ;
- **organiser et contrôler les livraisons.** Prévoir des équipements mobiles permettant de bloquer physiquement les véhicules appelés à pénétrer dans le périmètre le temps de ce contrôle ;
- apposer les affiches de sensibilisation à destination du public aux points d'entrées notamment « Réagir en cas d'attaque terroriste ».

Les véhicules-béliers constituent un mode d'action terroriste de plus en plus utilisé : attentats de Nice et de Berlin en 2016, attaque contre une patrouille de militaires à Levallois-Perret et attentats en Catalogne en 2017. Il est recommandé de mettre en place des moyens de circonstance permettant d'interdire l'accès au site ou de réduire la vitesse des véhicules à proximité des lieux de rassemblement. La mise en place de chicanes avec des obstacles successifs est également conseillée : plots en béton, bacs de fleurs de dimensions importantes, herses mobiles, barrières d'arrêt ou véhicules lourds (camions). Il est indispensable de tenir compte de la distance de pénétration potentielle d'un véhicule-bélier lors de la définition du périmètre extérieur d'un rassemblement (distance de sécurité entre les dispositifs de sécurité et la foule).

Exemple de revue de propagande de l'Etat Islamique qui préconise le recours à un véhicule-bélier.

2.3 - Au niveau des volumes intérieurs

- **désigner un responsable sûreté** qui sera l'interlocuteur unique des forces de l'ordre et des services d'incendie et de secours en cas d'intervention sur le site. Véritable coordinateur de la sûreté de l'événement, il doit connaître les bons réflexes à adopter. Il peut se rapprocher préalablement des forces de sécurité intérieure pour recueillir leurs conseils ;
- prévoir l'aménagement d'un **poste central de sûreté** au sein du site. Ce dernier doit être équipé 24H/24 par au moins un opérateur en mesure de visualiser les images du système de vidéo-protection mis en place ;
- **sécuriser la zone en période de fermeture du public** par la mise en œuvre d'un gardiennage humain ;
- **sensibiliser l'ensemble des collaborateurs au niveau de menace,** aux modes opératoires terroristes et à la détection de situations suspectes. Cette sensibilisation doit être complétée par une information sur les comportements à adopter en cas d'attaque.

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

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

Maquette et impression : Pôle Conception graphique-Fabrication – DSAF/DPL – Octobre 2017.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
MINISTÈRE DU TRAVAIL
MINISTÈRE DE L'ÉDUCATION NATIONALE
MINISTÈRE DES SPORTS

SECRÉTARIAT
GÉNÉRAL

Service spécialisé du haut fonctionnaire de défense et de sécurité
(SHFDS)

Paris, le 27 octobre 2017

Affaire suivie par : Loïc Le Gall
Courriel : HFDS@sg.social.gouv.fr
Tél. : 01 40 56 48 49
HFDS/UPDS/2017 - 141

NOTE

à l'attention de

MESDAMES ET MESSIEURS LES CONSEILLERS DE DEFENSE ET DE SECURITE DE ZONE,
LES DELEGUES DE DEFENSE ET DE SECURITE,
LES OFFICIERS ET RESPONSABLES DE SECURITE

Objet : Adaptation de la posture VIGIPIRATE « Transition 2017-2018 ».

Réf. : Partie publique du plan gouvernemental de vigilance, de prévention et de protection face aux menaces d'actions terroristes n°102000/SGDSN/PSN/PSE du 1er décembre 2016.
P. J. : - Annexe n°1 : « Tableau des mesures de vigilance » ;
- Annexe n°2 : « Ressources documentaires ».

VIGIPIRATE
SECURITE RENFORCEE
RISQUE ATTENTAT

Le niveau de vigilance « sécurité renforcée-risque attentat »
est maintenu sur l'ensemble du territoire national

La posture VIGIPIRATE « Transition 2017-2018 » s'applique à partir du **2 novembre 2017.** Elle prend en considération les vulnérabilités propres à la période de la fin d'année 2017 et du début d'année 2018. Elle s'applique, sauf événement particulier, jusqu'au **28 février 2018**.

Dans un contexte de menace terroriste très élevée, cette posture met l'accent sur :
- la sécurité des grands espaces de commerce lors des soldes d'hiver, des lieux de rassemblement, marchés de Noël notamment et des lieux de culte marqués par une forte affluence pendant les fêtes de fin d'année ;
- la sécurité dans le domaine des transports publics de personnes, en particulier lors des départs et retours des vacances scolaires et universitaires ainsi que dans les établissements d'enseignement, les établissements de santé, médico-sociaux et sociaux ;
- la protection des systèmes d'information face au risque d'attaque cybernétique.

I. Évaluation de la menace

La menace terroriste d'inspiration islamiste et jihadiste en France et contre nos ressortissants et intérêts à l'étranger **demeure à un niveau très élevé** et repose toujours principalement sur :

- **l'incitation** des partisans des groupes terroristes résidant sur le territoire national à commettre des actions isolées. Cela reste la principale menace ;
- **l'infiltration** d'opérationnels projetés depuis le Levant pour constituer des cellules terroristes. Les « revenants » représentent plutôt une menace à moyen terme, avec les revers que subit l'Etat islamique.

Dans ce contexte, **les cibles semblent déterminées principalement sur des critères d'opportunité**. Certains lieux ou événements représentent des cibles privilégiées : l'ensemble des grands rassemblements et événements à caractère symbolique (grands salons, célébrations religieuses, marchés de Noël, etc.), ainsi que les lieux publics très fréquentés (aéroports, transports urbains, lieux de divertissement, établissements commerciaux, etc.) ou au cœur du fonctionnement de notre société (écoles, hôpitaux, etc.).

S'agissant des **modes opératoires** employés ou susceptibles d'être utilisés, trois d'entre eux ont été privilégiés ces derniers mois :

- **le recours aux armes blanches ou autres moyens sommaires** (marteaux, machettes, etc.). Ces armes ont été utilisées dans la majorité des attaques en France en 2017 ;
- **les attaques au véhicule-bélier**, susceptibles d'entraîner un nombre élevé de victimes ;
- **l'utilisation d'engins explosifs improvisés ou de matières inflammables** (bouteilles de gaz, combustibles liquides), plusieurs projets terroristes déjoués récemment indiquent un intérêt accru des acteurs inspirés pour ce mode d'action.

D'autres modes opératoires sont régulièrement relayés par la propagande jihadiste :

- **les opérations de sabotage** des moyens de transport ferroviaire, aérien et routier ;
- **le risque associé aux sur-attentats** visant les forces d'intervention ou les attroupements générés lors de tels incidents. A cet égard, les hôpitaux recevant des blessés d'un premier attentat peuvent constituer une cible.

Les responsables de sites sont invités à sensibiliser leurs personnels à ces menaces et aux modes opératoires évoqués et à orienter leurs mesures de sécurisation dans ce sens.

II. Stratégie générale d'adaptation de la posture Vigipirate

Le **contexte général** de cette période est marquée par :

- **la sortie de l'état d'urgence et l'adoption du projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme**.

Cette loi dote les pouvoirs publics de nouveaux moyens juridiques en matière de prévention et de lutte contre le terrorisme.

La prise en compte de ces nouvelles dispositions se traduira par la création ou la mise à jour de fiches mesures du plan VIGIPIRATE, synthétisées dans le tableau en annexe 1.

Deux nouvelles mesures (**RSB 20-03** et **BAT 20-02**) y figurent par rapport à la posture précédente.

- **le maintien des contrôles aux frontières intérieures**. La France a rétabli les contrôles aux frontières intérieures le 13 novembre 2015. La réintroduction de ces contrôles devait expirer le 31 octobre 2017. Toutefois, en raison d'une menace terroriste qui demeure importante, la France a annoncé à la Commission européenne qu'elle prolongerait ses contrôles aux frontières jusqu'au 30 avril 2018.

- **l'évolution des modalités de déploiement des forces armées sur le territoire national**. La nouvelle articulation du dispositif Sentinelle permettra également de produire des efforts ciblés à l'occasion de grands événements susceptibles d'être pris pour cibles.

Plusieurs **axes d'effort** s'appliquent en matière de vigilance, de prévention et de protection. Ils tiennent compte de la multiplicité des cibles potentielles et de leur dispersion.

2.1 La vigilance dans les lieux accueillant du public et lors des rassemblements les plus sensibles

2.1.1. Mesures propres aux fêtes de fin d'année

La sécurité est renforcée autour des grands espaces de commerce pendant les fêtes de fin d'année et la période des soldes d'hiver (grands centres commerciaux, grands magasins, rues commerçantes et marchés de Noël). Lors des célébrations religieuses de fin d'année, la mise en œuvre de mesures de contrôle d'accès aux lieux de culte est recommandée en liaison avec les autorités religieuses locales.

2.1.2. Mesures permanentes

La capacité à faire face à une attaque terroriste dans les espaces de commerce, culturel et de loisir passe par le renforcement des échanges d'information entre les services de l'Etat et les responsables de la sûreté des opérateurs privés.

2.2 La sensibilisation des opérateurs et du grand public

Les services déconcentrés et les agences régionales de santé veilleront à ce que les opérateurs publics et privés dans leur champ de compétence mettent en place les logogrammes « Sécurité renforcée - risque attentat ».

Il est rappelé que les établissements recevant du public sont invités à adapter les mesures de sûreté qui leur incombent en fonction de la fréquentation saisonnière et à sensibiliser leurs personnels aux bons comportements à adopter en cas de situation suspecte, de menace d'attaque terroriste, de confinement ou d'évacuation selon les situations.

La sensibilisation de la population au signalement de tout comportement suspect doit être généralisée, car elle participe directement à la prévention de tout acte de terrorisme.

Une fiche de recommandations sur ce sujet est disponible sur le site Internet du SGDSN :
- http://www.sgdsn.gouv.fr/uploads/2017/07/fiche-signalement-situation-suspecte.pdf

En matière de prévention de la radicalisation, tout comportement suspect doit être signalé :
- http://www.stop-djihadisme.gouv.fr/ ou 0 800 005 696 (appel gratuit).

III. Adaptations particulières de la posture Vigipirate pour les ministères sociaux

Dans les champs d'activités des ministères sociaux, l'effort porte plus particulièrement sur :

3.1. La préparation et la mobilisation des moyens du système de santé

Les instructions[1] relatives au dispositif de préparation du système de santé visant à renforcer la réponse sanitaire aux attentats terroristes demeurent applicables par les établissements de santé.

[1] - instruction n°DGS/DUS/2016/42 du 19 février 2016 relative à la mise en œuvre de la feuille de route ministérielle visant à renforcer la réponse sanitaire aux attentats terroristes ;

Les agences régionales de santé (ARS) veilleront, d'une part, à bien articuler le schéma ORSAN AMAVI avec le plan ORSEC des préfectures et, d'autre part, à organiser le dispositif sanitaire des grands événements à sensibilité particulière selon les orientations des préfets.
A cet effet, un dialogue préparatoire sera systématiquement recherché avec les services préfectoraux, en lien avec les SAMU-Centre 15 territorialement compétents, pour assurer la préparation sanitaire en amont de tels évènements.

3.2. Les établissements de santé, sociaux et médico-sociaux

Les établissements de santé, sociaux et médico-sociaux demeurent des cibles potentielles particulièrement vulnérables.

Au sein des établissements de santé, les directeurs poursuivront leurs efforts de sécurisation de leurs sites en s'appuyant sur le déploiement de leur plan de sécurisation d'établissement (PSE) et la mise en œuvre d'actions de formation au profit de l'ensemble de leur personnel.
Les agences régionales de santé (ARS) renforceront le dialogue avec les préfectures sur la base des cartographies des établissements de santé qui viennent d'être réalisées.

Les établissements et services sociaux et médico-sociaux (ESSMS) s'attacheront à définir leur stratégie de protection pour la fin de décembre 2017, en s'appuyant sur les recommandations émises dans l'instruction n°SG/HFDS/DGCS/2017/219 du 26 juillet 2017 relative aux mesures de sécurisation dans les ESMS.
Les agences régionales de santé (ARS) et les directions régionales de la jeunesse, des sports et de la cohésion sociale (DR(D)JSCS) sont chargés de l'animation et de la coordination de la politique régionale de sécurité respectivement pour le secteur médico-social et le secteur social, en lien avec les conseils départementaux en cas de compétence conjointe.

3.3. Les établissements d'accueil du jeune enfant (EAJE) et les établissements relevant de la protection de l'enfance

La mise en œuvre des mesures préconisées dans la circulaire ministérielle n°DGCS/SD2C /2016/261 du 17 août 2016 sera poursuivie, notamment celles qui portent sur :
- les moyens de protection et le protocole de mise en sûreté des enfants et du personnel ;
- la formation du personnel et l'information des familles.

3.4. Les accueils collectifs de mineurs (ACM), les clubs sportifs et le secteur médico-éducatif

L'effort principal doit être dirigé sur la sécurisation des accès des ACM contre le risque d'intrusion et la procédure de signalement afférente. Les organisateurs et directeurs et animateurs en charge d'ACM pourront s'appuyer en particulier sur les mesures citées dans le guide joint en annexe 2.

Le renforcement de la vigilance doit être poursuivi dans les domaines de la sécurisation des espaces de rassemblement (intérieur, périphérie, périmétrie) et de l'organisation de manifestations (identification des vulnérabilités des évènements, gestion des flux,…).
Les organisateurs feront preuve d'un niveau élevé de vigilance lors des déplacements (embarquements, débarquements et transferts des publics concernés dans les cars, gares, ports et aéroports) et éviteront les regroupements de longue durée sur la voie publique.

- instruction interministérielle santé/intérieur du 4 mai 2016 relative à la préparation de situations exceptionnelles de type attentats multi-sites.
- note d'information du 11 avril 2017 complémentaire à l'instruction du 4 mai 2016 relative à la préparation des situations sanitaires exceptionnelles de type attentats multi-sites ;
- note d'information du 2 juin 2017 relative à la réponse opérationnelle des services d'aide médicale urgente et des services départementaux d'incendie et de secours pour la prise en charge des victimes d'attentats.

3.5. La sécurité des systèmes d'information

Une vigilance constante est à porter sur les systèmes d'information. L'application des mesures précisées en annexe 1 doit permettre de faire face aux menaces cyber et restent en vigueur.

Il est à noter que la période des fêtes est souvent une période d'accroissement des attaques. Traditionnellement, cette période est propice à l'échange massif de courriels et une baisse de vigilance, tant des utilisateurs que des équipes de sécurité numérique ; la sensibilisation de tous reste de mise.

Il est préconisé d'effectuer des rappels réguliers sur les risques liés aux « messages piégés », qui constituent le premier vecteur d'infestation virale, notamment de « rançongiciels ».

Il appartient aux organismes de surveiller leurs propres sites et de s'assurer de l'application des mesures proposées dans les guides d'hygiène informatique consultables sur les sites internet :
- de l'ANSSI : https://www.ssi.gouv.fr ;
- du centre de réponse aux attaques informatiques (CERT-FR) : https://www.cert.ssi.gouv.fr
- pour les établissements de santé du centre de cyberveille santé : https://www.cyberveille-sante.gouv.fr/

En cas d'incident, alerter la chaîne de sécurité des systèmes d'information des ministères sociaux :
- pour les établissements de santé, centre de radiothérapie et laboratoire de biologie sur le site de signalement des évènements sanitaires indésirables depuis l'espace dédié aux professionnels de santé : https://signalement.social-sante.gouv.fr
- pour tous les établissements non indiqués ci-dessus à l'adresse : ssi@sg.social.gouv.fr.

IV. Rappel de la vigilance lors des séjours l'étranger

Avant et durant tout déplacement à l'étranger, il est recommandé de :
- consulter, la rubrique « *conseils aux voyageurs* » sur le site du ministère de l'Europe et des affaires étrangères (MEAE), pour prendre connaissance des consignes de sécurité spécifiques au pays concerné :
  http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs.
- s'inscrire sur l'application *« Ariane »* quelle que soit la destination, y compris à l'intérieur de l'Union Européenne. Cette précaution permet à chacun d'être identifié comme présent dans la zone d'attentat et de recevoir des informations pratiques émanant du centre de crise et de soutien (CDCS) du MEAE pour tous les séjours hors de France :
  https://pastel.diplomatie.gouv.fr/fildariane/dyn/public/login.html

Ces mesures doivent **systématiquement être appliquées** par les encadrants de groupes de jeunes et d'équipes sportives se déplaçant à l'étranger.

Il vous est demandé de diffuser cette nouvelle posture à l'ensemble des correspondants de vos secteurs d'activités respectifs et de faire remonter au service spécialisé du HFDS des ministères sociaux les difficultés rencontrées dans son application (hfds@sg.social.gouv.fr).

Le haut fonctionnaire adjoint
de défense et de sécurité
Général (2s) Arnaud Martin

ORIGINAL SIGNE

ANNEXE 1

POSTURE « TRANSITION 2017-2018 »

TABLEAU DES MESURES DE VIGILANCE (1/3)

Action	Libellé mesure	Commentaires	N° mesure
Informer **Sensibiliser** **Informer** **Alerter**	Diffuser l'alerte au grand public	**RAPPEL** - Afficher le logo du niveau ***« sécurité renforcée-risque attentat »*** à l'entrée des sites accueillant du public.  Ces logos doivent être affichés à l'entrée et dans les espaces d'attentes des sites accueillant du public et peuvent être complétés d'une fiche synthétique récapitulant les conditions particulières de sécurité au sein de la structure. L'utilisation du logo ***« urgence attentat »*** fera l'objet d'instructions particulières en cas d'activation de ce niveau.  - Encourager et organiser la remontée des signes pouvant précéder une crise ou un attentat : comportements anormaux de personnes ou de véhicules, repérages, bagages ou colis abandonnés, etc. - Recommander le téléchargement de l'application pour Smartphone "Système d'alerte et d'information des populations" (SAIP) : http://www.gouvernement.fr/appli-alerte-saip	ALR 11-02 ALR 11-04
		- Sensibiliser le personnel aux mesures de cybersécurité, demeurer vigilant sur les courriels reçus, ne pas ouvrir les pièces jointes suspectes, limiter les navigations internet aux seuls rapports professionnels : *Guide d'hygiène informatique :https://www.ssi.gouv.fr/hygiene-informatique* Pour les établissements de santé : *https://www.cyberveille-sante.gouv.fr*	CYB

POSTURE « TRANSITION 2017-2018 »

TABLEAU DES MESURES DE VIGILANCE (SUITE 2/3)

Action	Libellé mesure	Commentaires	N° mesure
Surveiller Protéger	Renforcer la surveillance et le contrôle	***Manifestations en extérieur :*** Effort particulier de vigilance à porter : - aux activités sportives ; - aux activités et aux déplacements de groupes de mineurs. 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 ces obligations de sécurité du public ou des participants, soit en fonction de circonstances liées notamment à la thématique de la manifestation. Un contact avec les services de sécurité intérieure locaux est recommandé afin d'aider les organisateurs dans leur appréciation du risque.	RSB 11-01 RSB 12-01 RSB 13-01 **RSB 20-03** **(nouvelle mesure)**
	Restreindre voire interdire le stationnement et/ou la circulation aux abords des installations et bâtiments désignés	En lien avec les préfectures, renforcement de la vigilance sur les : - établissements de santé, médico-sociaux et sociaux ; - établissements d'accueil du jeune enfant (EAJE) et les établissements relevant de la protection de l'enfance.	BAT 11-02 BAT 12-02 BAT 13-02
	Renforcer la surveillance aux abords des installations et bâtiments désignés	La sensibilisation à la détection et au signalement de comportements suspects doit être réalisée.	BAT 11-03 BAT 12-03 **BAT 20-02** **(nouvelle mesure)**
	Renforcer la surveillance interne et limiter les flux (dont interdiction de zone)	Renforcement de la surveillance interne dans : - les établissements de santé, médico-sociaux et sociaux ; - les établissements d'accueil ; - les centres de loisirs - les bâtiments officiels. En s'appuyant sur les guides de bonnes pratiques. Pour les points d'importance vitale relevant du secteur santé : mise en application des plans particuliers de protection.	BAT 31-01
	Renforcer le niveau de sécurité des systèmes d'information	Pour les établissements de santé, mise en œuvre du plan d'action SSI décrit dans l'instruction SG/DSSIS/2016/309 du 14 octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information (« Plan d'action SSI ») dans les établissements et services concernés.	IMD 10-02

POSTURE « TRANSITION 2017-2018 »

TABLEAU DES MESURES DE VIGILANCE (SUITE 3/3)

Action	Libellé mesure	Commentaires	N° mesure
Surveiller Protéger	Renforcer la protection contre les intrusions dans les systèmes d'information Renforcer la protection contre les attaques en déni de service	Appliquer en priorité les mises à jour des postes utilisateur et les systèmes d'information utilisés ; Appliquer des règles de filtrage entre les réseaux (interne et externe) ; Limiter les impacts d'une attaque en déni de service, Mettre en place des sauvegardes régulières de toutes les données critiques. Élever la fréquence de sauvegarde à un niveau permettant la reprise des activités en cas d'altération des données.	CYB 42-01 CYB 42-02 CYB 43-01 CYB 43-02
Contrôler	Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier)	Contrôles renforcés aux accès des : - établissements de santé, médico-sociaux et sociaux ; - espaces de loisirs ; - établissements d'accueil du jeune enfant (EAJE) et les établissements relevant de la protection de l'enfance. *Les mesures de contrôle peuvent notamment consister en des dispositifs de filtrage et d'inspection visuelle des sacs.*	BAT 21-01 BAT 22-01 BAT 23-01
Alerter	Tenir à jour les inventaires des stocks de matières dangereuses pour détecter rapidement les vols ou disparitions et signaler ces disparitions aux autorités	Signaler tous vols, disparitions ou transactions suspectes de précurseurs d'explosifs et agents NRBC au point de contact national : - pôle judiciaire de la gendarmerie nationale : pixaf@gendarmerie.interieur.gouv.fr Tél H/24 : 01.78.47.34.29. et au service spécialisé du HFDS : hfds@sg.social.gouv.fr	IMD 10-01
	Alerter des incidents sur les systèmes d'information	Signaler tout incident de sécurité sur les systèmes d'information à l'adresse : ssi@sg.social.gouv.fr Pour les établissements de santé, centre de radiothérapie et laboratoires de biologie sur le site signalement des évènements sanitaires indésirables depuis l'espace dédié aux professionnels de santé : https://signalement.social-sante.gouv.fr	CYB
Protéger les structures de santé	Protéger les établissements de santé	Les directeurs des établissements de santé doivent poursuivent les efforts de sécurisation de leurs sites en s'appuyant sur le déploiement de leur plan de sécurité d'établissement (PSE), le renforcement des relations avec les préfectures et les forces de sécurité intérieure et la mise en œuvre d'actions de formations à l'intention de l'ensemble de leur personnel.	SAN 50-01

NB : Les mesures sont numérotées avec les critères suivants :

- trigramme de domaine :

ALR : Alerte	BAT : Installations et bâtiments
CYB : CYBER	IMD : Installations et matières dangereuses
RSB : Rassemblements et zones ouvertes au public	SAN : Santé

- numéro d'ordre (dans le tableau du plan Vigipirate) de la mesure de 01 à 0x pour les mesures du socle et de 01 à 0x pour les mesures additionnelles.

Exemple : la mesure BAT 13-04 : est une mesure du secteur installations et bâtiments (BAT), s'inscrit dans le 1er objectif du secteur (adapter la sûreté externe).

Annexe 2

RESSOURCES DOCUMENTAIRES

I. GUIDES DE BONNES PRATIQUES ET DES REFERENTIELS ADAPTES AUX SECTEURS D'ACTIVITES DES MINISTERES SOCIAUX DISPONIBLES ET TELECHARGEABLES SUR INTERNET

- http://www.sgdsn.gouv.fr/vigipirate
- http://www.interieur.gouv.fr/actualuites/L-actu-du-Ministère/Publication-du-guide-gérer-la-surete-et-la-securite-des-evenements-et-sites-culturels
- http://solidarites-sante.gouv.fr/IMG/pdf/guide_securisation_batiments.pdf

II. ETABLISSEMENTS DE SANTE, SOCIAUX ET MEDICO-SOCIAUX

Les directeurs de ces établissements pourront s'appuyer respectivement sur :
- un guide d'aide à l'élaboration du plan de sécurisation d'établissement de santé ;
- un outil d'auto-évaluation de sûreté et un modèle de fiche de sécurité pour les ESSMS.

Ces différents supports sont disponibles en téléchargement sur le site du ministère des solidarités et de la santé : http://solidarites-sante.gouv.fr/ministere/defense-et-securite-hfds/article/plans-de-defense-actions- de-prevention-gestion-de-crise

III. ETABLISSEMENTS D'ACCUEIL DU JEUNE ENFANT ET ETABLISSEMENTS RELEVANT DE LA PROTECTION DE L'ENFANCE

Les gestionnaires de site pourront s'appuyer sur les mesures préconisées dans les guides de bonnes pratiques à destination des chefs d'établissement et des directeurs d'école :
- http://www.gouvernement.fr/reagir-attaque-terroriste
- http://www.education.gouv.fr/vigipirate

Ainsi que sur le guide « Sûreté dans les établissements d'accueil du jeune enfant, se préparer et faire face aux situations d'urgence particulière » (avril 2017).
http://solidarites-sante.gouv.fr/IMG/pdf/final_mise-a-jour_24-avril_guide-securite_eaje.pdf

IV. ACCUEILS COLLECTIFS DE MINEURS

Les organisateurs, directeurs et animateurs en charge d'accueils collectifs de mineurs à caractère éducatif pourront s'appuyer sur les mesures préconisées dans :
- le guide vigilance attentats les bons réflexes : « accueil collectifs de mineurs » à destination des organisateurs, des directeurs et des animateurs en charge d'accueils collectifs de mineurs à caractère éducatif (janvier 2017) ;
  http://www.jeunes.gouv.fr/actualites/zoom-sur/article/guide-vigilance-attentats-accueil
- les mesures générales de vigilance, de prévention et de protection :
  http://www.gouvernement.fr/reagir-attaque-terroriste