PREMIER
MINISTRE

Liberté
Égalité
Fraternité

VIGIPIRATE

FAIRE FACE ENSEMBLE

GUIDE DES BONNES PRATIQUES POUR LA SÛRETÉ DES ESPACES PUBLICS

Secrétariat général de la défense
et de la sécurité nationale

ÉDITORIAL

Les séries d'attentats qui se sont succédé sur notre territoire depuis 2015 sont le reflet d'une menace particulièrement élevée en Europe. Elles sont souvent perpétrées au nom d'idéologies radicales, islamistes particulièrement. Malgré l'affaiblissement des organisations terroristes et la dégradation importante de leurs capacités à projeter des attaques sur notre sol, cette menace terroriste se maintient à un niveau élevé. Ainsi, en 2020 et 2021, ce ne sont pas moins de sept attaques terroristes abouties qui ont causé la mort de huit personnes en France.

Si une attaque peut être conduite en tout lieu du territoire, les transports, les grands rassemblements festifs, les sites symboliques, les lieux publics très fréquentés, les établissements de santé, écoles, universités ou administrations publiques et privées sont particulièrement ciblés. Dans ce cadre, le SGDSN a souhaité développer un **guide des bonnes pratiques pour la sûreté des espaces publics**, destiné à tous les exploitants et usagers d'établissements recevant du public, ainsi qu'aux élus locaux et aux représentants de l'État.

Il est conçu avec l'ambition de diffuser une culture de la sécurité auprès de nos concitoyens. L'acuité de cette ambition se reflète par l'organisation en France de grands évènements internationaux, tels que les Jeux Olympiques en 2024. Ce guide concourt donc à trois grands objectifs : **sensibiliser** à la menace terroriste ; **aider les responsables** de lieux accueillant du public à l'anticiper et à déployer les moyens adaptés ; **présenter les réactions** et gestes réflexes susceptibles d'être adoptés en cas d'attaque. Élaborées en étroite collaboration avec les hauts fonctionnaires de défense et de sécurité des ministères, les recommandations de ce guide s'appliquent à tous les espaces publics et prennent en compte toutes les menaces. En effet, elles ciblent aussi bien les modes opératoires rudimentaires que sophistiqués comme l'utilisation de substances chimiques ou biologiques.

Ce guide, disponible en ligne, sera régulièrement mis à jour en fonction du contexte sécuritaire et du cadre juridique. Il nous permet de renforcer notre vigilance et de nous adapter constamment à l'évolution des menaces. Il complète utilement la plateforme Vigipirate « Faire face ensemble ».

Le Préfet, Directeur de la protection et de la sécurité de l'État

Nicolas de MAISTRE

GUIDE DES BONNES PRATIQUES POUR LA SÛRETÉ DES ESPACES PUBLICS

SOMMAIRE

Le plan VIGIPIRATE 5

Le guide 6

I. Analyse générale de la menace 7

Menaces 8

Vulnérabilités : des cibles privilégiées 9

Modes d'action. 10

II. Fiches sectorielles. 11

Sécurisation des transports 12

Sécurisation des établissements de santé 15

Sécurisation des lieux culturels 18

Sécurisation des lieux de culte. 20

Sécurisation des magasins et centres commerciaux. 22

Sécurisation des administrations publiques et privées 24

Sécurisation des grands rassemblements extérieurs 26

Sécurisation des grands rassemblements intérieurs 28

Sécurisation des sites touristiques 30

Sécurisation des hôtels et restaurants 32

Sécurisation des lieux de vie nocturne 35

Sécurisation des écoles et des établissements scolaires 38

Sécurisation des établissements d'enseignement supérieur et de recherche . 41

III. Fiches procédurales 44

Organisation et anticipation 45

OA1 Mise en place d'un plan de sécurisation de l'établissement (PSE) . . . 46
OA2 Formation et sensibilisation du personnel 49
OA3 Organisation d'un exercice de sûreté 50
OA4 Chaîne d'alerte face à une menace 62
OA5 Vérification du personnel 65
OA6 Préparer sa communication de crise 70
OA7 Conseils aux voyageurs 75

Réaction 78

R1 Réaction | Prévenir les autorités 79
R2 Réaction | Attaques armées 81
R3 Réaction | Prise d'otages 85
R4 Réaction | Produits toxiques 86
R5 Réaction | Drones malveillants 90
R6 Réaction | Cyberattaque 92
R7 Réaction | Signalement d'un individu suspect 94
R8 Réaction | Fouille des locaux 99

Moyens 100

M1 Moyens | Mise en place d'un système de vidéosurveillance 101
M2 Moyens | Mise en place d'un système de contrôle des accès 107
M3 Moyens | Mesures d'entraves aux véhicules béliers 110
M4 Moyens | Mise à niveau de la sécurité des systèmes d'informations . . . 112

Pour aller plus loin 118

LE PLAN VIGIPIRATE

Le plan VIGIPIRATE, créé dès 1978 en réaction à l'attaque de l'aéroport d'Orly par des terroristes palestiniens, vise à organiser le dispositif français de lutte contre le terrorisme. Piloté par le Premier ministre, ce plan associe secteur public, secteur privé, collectivités territoriales et citoyens et vise, outre la vigilance, deux objectifs :

La protection, en assurant en permanence une protection adaptée des citoyens, du territoire et des intérêts de la France contre la menace, en France comme à l'étranger. Après une analyse de l'état de la menace terroriste, le plan Vigipirate permet l'activation d'un certain nombre de mesures graduées.

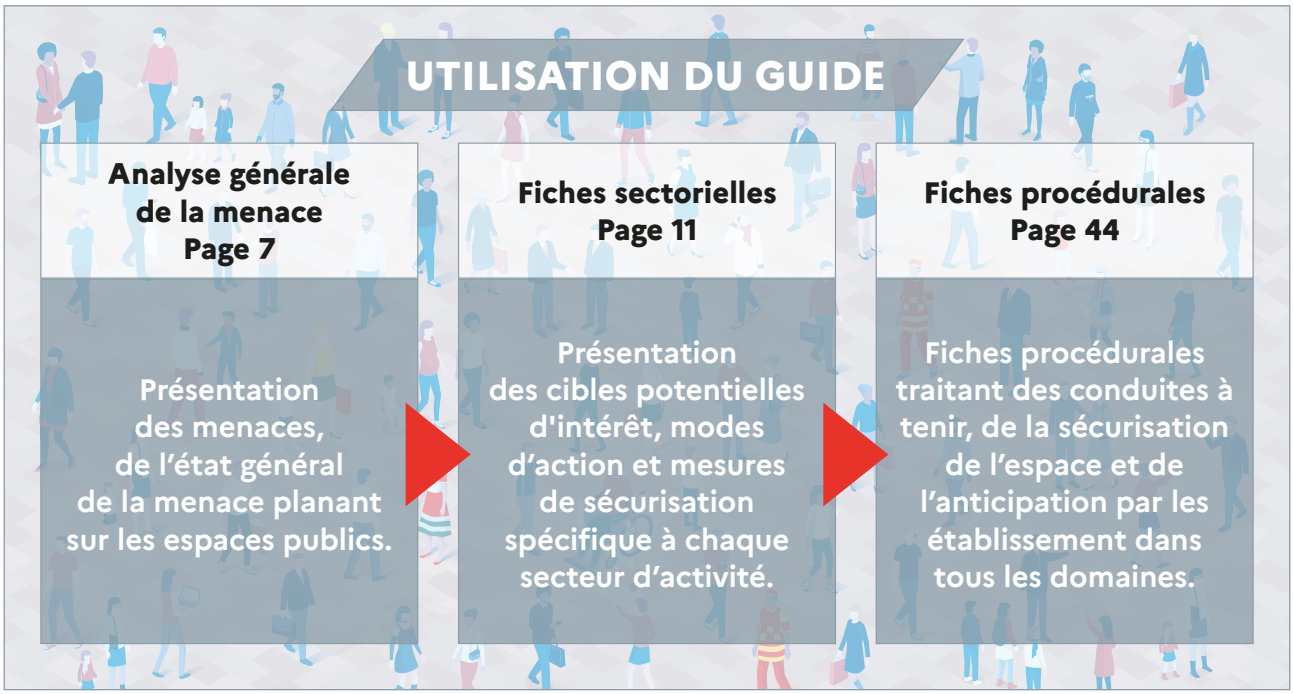
La sensibilisation, en développant une culture de la vigilance et de la sécurité dans l'ensemble de la société, afin de prévenir ou développer, le plus en amont possible, toute menace d'action terroriste. À ce titre, le plan Vigipirate s'inscrit dans la continuité du Plan d'action contre le terrorisme (action n°14 promouvant le « développement d'une culture commune de la sécurité au sein de la société ») et prend part à une démarche nationale de résilience face aux risques planant sur les espaces publics.

LE GUIDE

Face au niveau de la menace, l'action publique ne peut être efficace sans le concours de la société civile. Les exploitants d'établissements recevant du public (ERP) et les représentants politiques locaux ont donc une responsabilité pénale et morale dans la mise en œuvre de mesures de sécurité. Ce vade-mecum vise donc à leur fournir, ainsi qu'à toute autre personne susceptible de contribuer à la sécurisation des espaces publics, les informations et les procédés inhérents au besoin de vigilance, en complément du plan VIGIPIRATE. Il est ainsi structuré en trois parties :

- la première, présentant une analyse de la menace planant sur les espaces publics,
- la deuxième, composée de **fiches spécifiques à chaque secteur d'activité.** Les menaces spécifiques, cibles spécifiques, modes d'actions privilégiés et mesures relatives à la sécurisation des espaces publics, domaine par domaine, y sont présentés.
- la dernière, consiste à rassembler un ensemble de **fiches procédurales** traitant des conduites à tenir, de la sécurisation de l'espace et de l'anticipation par les établissements dans tous les domaines. Des fiches réflexes sont également fournies pour aider à mettre en place et maintenir en condition les divers systèmes et procédures de sécurité.

Après la lecture de l'état général de la menace, un rappel sur les spécificités et enjeux propres à certains domaines d'activité est présenté. Ensuite, les fiches thématiques aideront de manière très concrète à sécuriser les établissements et à instaurer les procédures nécessaires en cas de péril imminent.



I.
ANALYSE GÉNÉRALE DE LA MENACE

Menaces

La France est confrontée à une menace terroriste durablement élevée et les risques planant sur les espaces publics sont de natures et de sources diverses. Bien que susceptibles d'évoluer, les menaces contemporaines peuvent être classées en trois catégories suivant leurs spécificités :

Depuis 2015, la France a été visée à plusieurs reprises par des **organisations terroristes** animées par une idéologie islamiste sunnite, mortifère et expansionniste. Ces dernières cherchent à atteindre le monde occidental en organisant des attaques terroristes aux modes opératoires variés et évolutifs, perpétrées par des individus endoctrinés. Le caractère principalement endogène de cette menace la rend plus difficile à détecter et donc à neutraliser. De plus, les terroristes islamistes en France bénéficient de l'expertise des combattants djihadistes en Irak et au Levant. Ils sont ainsi à même de développer continuellement de nouvelles formes d'attaques adaptées à nos mesures de sécurité et encouragées par leur propagande. De ce fait, leur capacité de nuisance est considérable et doit être prise au sérieux tant par les services de l'État que par la société civile.

Par ailleurs, d'autres mouvements se nourrissant des tensions créées par le terrorisme islamiste prennent de l'ampleur et représentent désormais un danger sérieux. **Ultra-gauche et ultra-droite** sont toutes deux considérées comme des risques émergents. Les actions violentes de l'ultra-gauche se concentrent principalement sur les institutions, avec la volonté de renverser le système économique, politique et social établi. À l'opposé du spectre, les groupuscules d'ultra-droite nationalistes s'inscrivent dans une rhétorique islamophobe et xénophobe.

Enfin, les attaques dont les auteurs présentent des **troubles psychiatriques** se multiplient. S'il est difficile d'établir un profil-type tant les causes pathologiques varient, la similarité des modes opératoires avec les catégories précédentes impose d'appliquer les mêmes logiques préventives et réactives de sécurité. De plus, les rhétoriques ou les passages à l'acte des groupes terroristes peuvent être des éléments déclencheurs du passage à l'acte chez des individus psychologiquement fragiles.

Dans la plupart des cas, ces individus malveillants cherchent à atteindre des cibles faciles d'accès et dont les potentielles nombreuses victimes ou la charge symbolique permettront un retentissement majeur de leur cause. À ce titre, les espaces publics représentent une cible privilégiée. Si l'ensemble des mesures préconisées dans ce vade-mecum vise principalement à entraver des actions terroristes, leur application permet naturellement de réduire les risques inhérents à la criminalité (braquages, cambriolages, agressions physiques, etc.) ou aux envahissements violents (mouvements sociaux).

Vulnérabilités : des cibles privilégiées

Un espace public est défini dans le droit français comme « un lieu accessible à tous, sans autorisation spéciale de quiconque, que l'accès en soit permanent et inconditionnel ou subordonné à certaines conditions »[1]. Les terroristes ont clairement exprimé leur intérêt pour ces derniers comme cibles stratégiques, tant en France qu'à l'étranger, car leurs caractéristiques s'alignent sur les objectifs des terroristes :

- Une **forte charge symbolique :** leur nature culturelle, politique, économique, sociale ou cultuelle peut amplifier l'impact d'une attaque. En outre, tout un chacun peut se sentir directement visé dans l'attaque d'un espace que l'on a l'habitude de fréquenter. Au-delà de l'impact physique de l'attentat, sa portée psychologique à l'échelle de la société donne une dimension particulière au discours revendiqué.
- Par définition ouverts à l'ensemble de la population, ils sont **faciles d'accès.** Des mesures strictes de sécurité étant difficilement compatibles avec leurs vocations initiales, ces espaces publics sont une solution de facilité pour la mise en œuvre d'une attaque terroriste.
- De par leur fréquentation quasi-continue avec des pics d'intensité à certaines périodes (périodes de soldes, heures de pointe, etc.), les espaces publics peuvent **concentrer une foule dense** et donc permettre la maximisation du nombre de victimes sur une fenêtre spatio-temporelle réduite.

Il existe également des menaces ou des spécificités propres à chaque lieu public (commerces, gares, université, lieux de culte, cinémas, etc.). Ce document intègre donc des éléments précis, secteur par secteur, rédigés par les Hauts Fonctionnaires de Défense et de Sécurité (HFDS) des ministères de tutelle.

1 TGI de Paris, 23 octobre 1986, confirmé par un arrêt de la Cour d'appel de Paris du 19 novembre 1986.

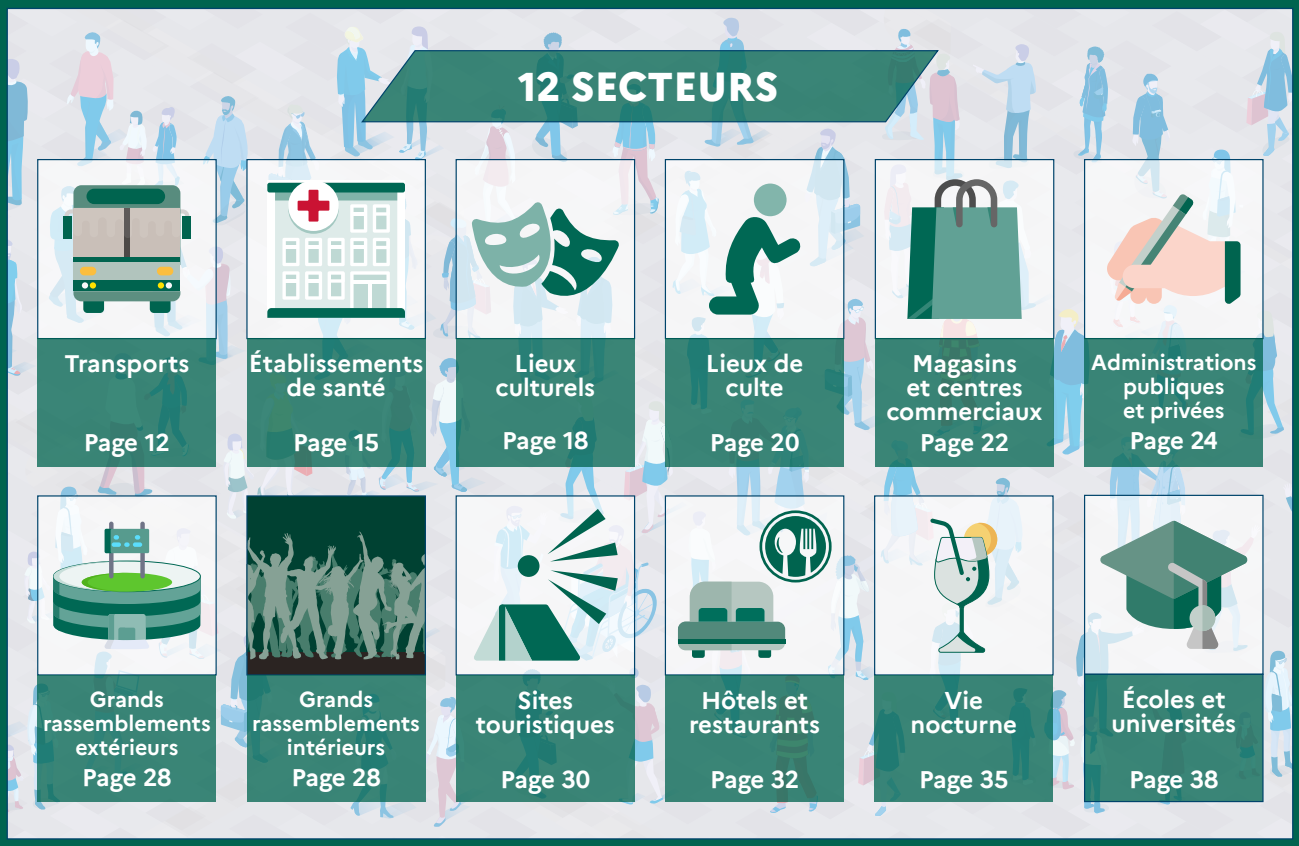
Modes d'action

Les espaces publics ont été particulièrement visés ces dernières années, avec des modes opératoires variés et fortement susceptibles d'évoluer avec le progrès technique et la recomposition de la menace. Certains modes d'action sont susceptibles d'être mis en œuvre par les terroristes :

- **L'attaque à main armée aux moyens d'armes de guerre** (fusils d'assaut, grenades, etc.) ou d'armes blanches (machette, couteau de cuisine, etc.) qui occasionne de lourdes pertes humaines.
- **L'utilisation d'explosifs,** dissimulés dans des bagages, des véhicules ou sur des personnes et qui affectent indistinctement les personnes et les bâtiments.
- **L'attaque par un véhicule bélier :** une voiture ou un camion qui percute la foule, des véhicules ou un bâtiment à grande vitesse.
- L'exposition de la population à un **agent toxique** de nature nucléaire, radiologique, biologique ou chimique par divers procédés (empoisonnement de l'eau, accès aux réseaux de ventilation, etc.)
- L'utilisation d'un **drone malveillant** que ce soit pour préparer une attaque en repérant les lieux ou en transportant directement une charge explosive/NRBC.
- **L'attaque des systèmes d'informations** (ou cyberattaque), qui vise à déstabiliser ou interrompre les activités d'une structure. Bien que l'impact soit principalement économique ou capacitaire, une attaque informatique peut aboutir à des pertes humaines en fonction des organismes visés.

De la même manière que pour les cibles, certains secteurs d'activité sont plus susceptibles d'être confronté à un type d'attaque qu'à un autre. Afin de mieux vous accompagner dans la sécurisation de votre établissement, ce guide intègre des précisions adaptées à celui-ci.

II. FICHES SECTORIELLES



SÉCURISATION DES TRANSPORTS

Le domaine des transports regroupe les transports terrestres (routiers et ferroviaires), maritimes, fluviaux et aériens. Il différencie la sécurité, qui a pour objet de prévenir la survenance d'un accident dû à des défaillances, matérielles ou humaines, ou à des causes naturelles et la sûreté, qui vise à protéger les personnes et les biens transportés, les matériels et installations liés à l'exploitation contre des actes de malveillance (terrorisme, criminalité, délinquance, etc.), par une combinaison de mesures organisationnelles et de moyens matériels ou humains. Bien que le terrorisme ne soit pas un phénomène récent et que des mesures soient mises en place pour préserver ou renforcer la sûreté, des efforts considérables ont été réalisés pour améliorer celle-ci à la suite d'événements majeurs, parmi lesquels les attentats du 11 septembre 2001. Dans ce contexte, les acteurs concernés veillent au maintien de la sûreté des transports pour deux raisons : d'une part, nombre d'infrastructures et de véhicules de transport constituent des cibles de choix pour une attaque terroriste en raison de la concentration de victimes potentielles ; d'autre part, les transports peuvent être utilisés comme vecteurs d'attaques terroristes, par exemple en permettant l'entrée d'armes au niveau des ports ou le détournement d'avions à des fins meurtrières. Dans tous les cas, la difficulté de protéger les nombreuses cibles potentielles tout en préservant la fluidité de fonctionnement des transports accentue l'intérêt que présentent ceux-ci en tant que cibles. Cette fiche vise à préciser les enjeux liés au transport vis-à-vis de la menace terroriste.

Les menaces et cibles spécifiques

Les attentats terroristes ciblent particulièrement le secteur des transports depuis le début des années 80 aussi bien en France que dans le reste de l'Europe et du monde. Ils sont souvent perpétrés dans les gares, les trains ou les aéroports. À titre d'exemple, on peut citer les attentats de : Moscou et Madrid en 2004, Londres en 2005, Francfort en 2011, du Train Thalys en 2015, de Bruxelles en 2016, Londres et Marseille en 2017, Utrecht (Pays-Bas) en 2019, etc. Ces quelques exemples illustrent l'attrait que les terroristes ont pour ces cibles ouvertes à la population et pouvant faire de nombreuses victimes dans des espaces restreints ou clos.

Les infrastructures et les vecteurs de transport présentent une caractéristique commune : ce sont des lieux avec de fortes concentrations de personnes, surtout aux heures de pointe et facile d'accès. Par ailleurs, ces infrastructures abritent fréquemment des centres commerciaux, qui entraînent également des flux de personnes importants et dont la sûreté est, dès lors, menacée.

Ces structures sont donc vulnérables en raison de l'importance des flux qui y transitent chaque jour. Des terroristes pourraient actionner une charge explosive ou de sortir une arme pour faire feu. Ces opérations qui visent des lieux publics avec une forte affluence présentent pour leurs auteurs un rapport coûts/bénéfices qui est considérable. Dans ce cadre, les infrastructures de transports publics constituent des cibles potentielles.

Les gares ferroviaires et stations de métro, les réseaux ferrés, ainsi que les matériels qui y circulent sont par nature vulnérables à la menace terroriste telle qu'elle est identifiée aujourd'hui (attentats à la bombe, recours à des armes automatiques ou chimiques). Ces endroits ont toujours été conçus comme des espaces ouverts, avec de multiples accès. Cette facilité d'accès et de circulation est un gage d'attractivité pour les transports ferrés. La faculté offerte aux voyageurs de circuler librement avec leurs bagages rend en outre particulièrement complexe la différenciation entre un simple colis délaissé et un colis suspect.

Par ailleurs, ces espaces, notamment les centres commerciaux, sont souvent particulièrement étendus, répartis sur plusieurs niveaux, et n'ont en général pas été, à l'origine, conçus en tenant compte des aspects liés à la sûreté face à la menace terroriste.

Modes d'action privilégiés

Il apparaît que les attaques récurrentes contre le secteur des transports soient perpétrées par : l'usage **d'explosifs**, des **armes** (blanches ou à feu) et des **armes par destination** (détournements de vecteurs de transport : avion, train, bus, bateau).

Ce phénomène est inhérent au monde des transports du fait : de l'ouverture des accès des infrastructures et notamment des vecteurs ferroviaires et des flux massifs qui les empruntent quotidiennement.

Les modes d'actions (MA) pourraient être :

- Une attaque **NRBC** (ex : par gaz) dans les emprises de transport aux heures de pointe,
- Une arme par destination visant des populations nombreuses,
- Des bombes placées sur une voie ferrée faisant dérailler un mobile.
- Une **cyberattaque** dans le système d'information d'un opérateur de transport.

Mesures préventives et réactives

Des mesures de prévention visent à prévenir les actes de malveillance notamment par :

- **La formation et la sensibilisation** des agents de terrain sur ces sujets,
- L'augmentation des patrouilles de sécurité dans les emprises (PN, GN, services internes de sécurité, sentinelle),
- La mise en place de services de médiation et de partenariats locaux,
- La généralisation de l'utilisation de la **vidéoprotection** dans les emprises et dans les vecteurs de transports terrestres,
- Les procédures spécifiques en cas de découverte d'un **colis abandonné / suspect**.

Le SHFDS du MTE traite spécifiquement les questions relatives à la sûreté (à la malveillance en général et au terrorisme en particulier) avec :

- Les délégués à la défense et à la sécurité des opérateurs d'importance vitale,
- Les personnes en charge des questions de sûreté des opérateurs,
- Les directions de la sûreté des opérateurs.

Liens utiles

Sécurité et transports routiers | ecologie.gouv.fr

Sécurité maritime et sûreté maritime | ecologie.gouv.fr

Les acteurs de la sécurité ferroviaire | ecologie.gouv.fr

SÉCURISATION DES ÉTABLISSEMENTS DE SANTÉ

Les établissements de soins, tant en France qu'à l'étranger, sont fréquemment confrontés à des actes de malveillance allant de l'incivilité à l'acte terroriste. Penser la sécurisation des établissements de santé face aux violences qui s'exercent contre les professionnels de santé ou face aux risques d'attentats ou de sur-attentats, nécessite une approche globale. Cette dernière doit permettre le renforcement de la sécurité, tout en garantissant la qualité de l'offre de soins, l'accueil des usagers et la qualité de vie au travail des personnels de santé. Il s'agit plus largement de développer chez les professionnels de santé une culture permanente de la gestion du risque et de la sûreté, afin qu'ils s'impliquent pleinement dans cet enjeu majeur pour la résilience de l'établissement.

Les menaces et cibles spécifiques

Les établissements de santé, tout comme les établissements sociaux et médico-sociaux, sont soumis à une complexité intrinsèque liée aux multiples dispositions réglementaires et normatives sur les plans techniques et organisationnels. Ils doivent également intégrer des objectifs d'efficience.

Ainsi, parmi l'ensemble des établissements recevant du public, le fonctionnement des établissements de santé doit répondre à un ensemble de spécificités à la fois complexes et atypiques liées :

- À l'hétérogénéité du public (personnels, usagers, familles, sous-traitants, etc.) et à certaines caractéristiques particulières (personnes vulnérables et dépendantes qui peuvent être peu ou pas mobiles) ;
- À la prise en charge des personnes soignées, qui impose une continuité des activités de soins ;
- Aux aménagements intérieurs, qui comportent de nombreuses sources de risques (chimiques, explosifs, biologiques, radiologiques, etc.) ;

- Aux systèmes d'informations numériques multiples et aux finalités différentes mais le plus souvent interconnectés (GTC, GTB, biomédical, IdO-IoT[2], etc.) ;
- Aux aménagements extérieurs, qui comportent de nombreuses sources de risques (attaques par véhicules bélier sur les parvis et voies piétonnes d'accès, accès non filtrés dûs à l'ouverture sur la ville, etc.).

À ce titre, les établissements présentent des vulnérabilités particulières liées aux flux, dont la gestion doit être impérativement coordonnée, structurée et adaptée à leur configuration et leur finalité :

- Contrôle des flux de personnes et de véhicules : personnels de santé, visiteurs, usagers (notamment en cas d'afflux massifs) ;
- Contrôle des flux quotidien des véhicules : personnels de santé, visiteurs, usagers, véhicules de secours ;
- Gestion des flux d'information et de communication (réseau téléphonique et informatique, données des personnes soignées, etc.) ;
- Gestion des flux logistiques et des prestataires de service (matériel médical, matières dangereuses, fluides médicaux, lingerie, nourriture, véhicules et piétons, etc.).

Modes d'action privilégiés

Du fait de ces vulnérabilités, l'offre de soins est exposée à certains risques. Il peut notamment s'agir de :

- **Intrusions :**
  - Sabotage, détérioration ou destruction d'installations, tir d'armes diverses ou incendie ;
  - Enlèvement (nourrisson, etc.), prise d'otages, évasion d'un détenu ;
  - Vol d'équipements sensibles ou de produits de santé ;
  - **Drone malveillant** ;
  - Blocage d'accès à un site empêchant son activité ;
- **Atteintes numériques :**
  - Sabotage (en particulier SI liés aux matériels biomédicaux, au contrôle d'accès, à la gestion technique centralisée (GTC) et à la gestion technique de bâtiment (GTB).
  - Propagation de virus ou autres codes malveillants (rançongiciel) portant atteinte à l'intégrité des données (dossiers de usagers, résultats médicaux, matériel biomédical, archives légales) ;
  - Perturbation dans la fourniture de télécommunications, d'énergie ou de fluides ;
  - Intrusion dans les systèmes d'informations
- **Violences :**
  - Risques liés à certaines pathologies des personnes soignées (psychiatrie, urgences, neurologie, gériatrie, etc.) : agressions physiques et psychologiques, disparitions mettant en danger les personnes, comportements suicidaires ;
  - Risques liés aux comportements des personnes soignées, d'accompagnants, d'intrus et de SDF : violences à main nue, avec arme, règlement de compte entre bandes, actes de malveillance ;
- **Attentat :**
  - **À l'arme blanche**, balistique, **explosif**, **véhicule bélier**, **NRBC**, etc. ;

2 Internet des objets (IdO) - Internet of Things (IoT) : dont les objets connectés en santé.

Mesures préventives et réactives

La multiplication de ces risques impose une vigilance accrue et nécessite - afin d'en limiter la portée - d'assurer sur l'ensemble du territoire la prise en compte effective de mesures particulières de sûreté au sein des structures de « santé ». Élaborée par le SHFDS des ministères sociaux, cette démarche est pilotée par les directeurs généraux des agences régionales de santé, en coordination avec les préfets de département, les forces de sécurité intérieure et le dispositif du plan gouvernemental de vigilance, de prévention et de protection « Vigipirate ».

Ce guide est ainsi un outil à disposition des directeurs d'établissements et de leurs équipes pour les aider et les accompagner dans l'élaboration et la mise en œuvre de leur PSE, notamment par :

- Le renforcement de la **protection de leur établissement**, tant contre les violences au quotidien que contre la menace terroriste, aujourd'hui multiforme ;
- La réalisation d'un diagnostic de sécurité (cartographie des risques et acteurs);
- Le renforcement de la coordination à l'échelon départemental, entre le responsable de l'établissement et le préfet, le procureur de la République, les forces de sécurité intérieure (*via* les référents sûreté) et les élus.

Ce guide fourni ainsi des fiches-conseils sur les conduites à tenir face à des évènements présentant des risques, tant pour le personnel que pour l'établissement. Il conviendra d'insister sur la nécessaire **sensibilisation du personnel**, sur son rôle en matière de vigilance et de prévention et aux conduites à tenir en cas de violence, de malveillance et d'attentat sur site ou dans l'environnement immédiat de l'établissement.

Par ailleurs, des documents opérationnels et spécifiques aux établissements de santé rédigés par le ministère de la santé en lien avec d'autres services de l'État sont accessibles sur demande auprès de votre agence régionale de santé.

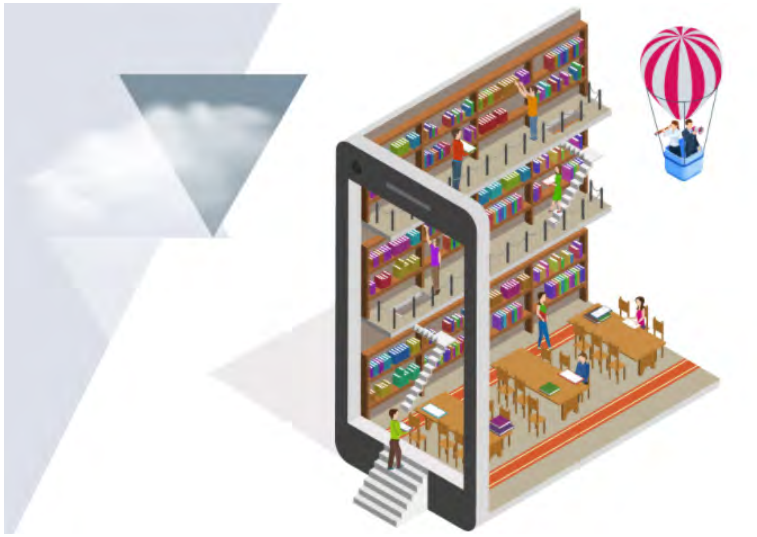
Liens utiles

Guide d'aide à l'élaboration d'un PSE | solidarites-sante.gouv.fr

Sécurité sanitaire réglementation applicable dans les établissements de santé | solidarites-sante.gouv.fr

Sécurisation des établissements de santé | ars.sante.fr

SÉCURISATION DES LIEUX CULTURELS



Les menaces et cibles spécifiques

Les sites, événements et établissements culturels sont par essence extrêmement exposés à la menace terroriste d'inspiration islamiste. Lieux de vie, de partage et de création, ils ont une valeur symbolique forte tant du point de vue de l'histoire de notre pays que de celui de la valorisation d'un mode de vie occidental régulièrement visé par les terroristes. Les salles de spectacles ont été à plusieurs reprises visées tant en France (Bataclan, Paris, 13 novembre 2015) qu'à l'étranger (Concert d'Ariana Grande, Manchester, Royaume-Uni, 22 mai 2017). Les entreprises de presse (Charlie Hebdo, Paris, 7 janvier 2015 et 25 septembre 2020) ont aussi été touchées. Les attaques contre les musées concernent aussi la France (Carrousel du Louvre, Paris, 3 février 2017) et ses partenaires étrangers (Musée du Bardo, Tunis, Tunisie, 18 mars 2015). Les monuments historiques affectés à un culte sont aussi des cibles clairement identifiées (attentat de Saint-Étienne du Rouvray le 26 juillet 2016, attentat sur le parvis de Notre-Dame de Paris le 6 juin 2017, tentative d'attentat à la voiture piégée à proximité de Notre-Dame de Paris le 4 septembre 2016 et attentat de Nice le 29 octobre 2020) et font l'objet d'une **fiche sectorielle détaillée**. Les lieux de création ou de diffusion, voire certains lieux de conservation de la mémoire nationale, peuvent également être la cible d'attaques de la part de groupes violents aux motivations politiques ou religieuses.

Par ailleurs, outre les fêtes religieuses, les événements culturels majeurs (festivals notamment) par le nombre important de spectateurs qu'ils attirent présentent une certaine sensibilité. Les expositions mettant en avant des œuvres de nature à choquer certains groupes ou personnes appellent aussi à la vigilance. Le recours à certains mécènes controversés peut également inciter des groupes violents à passer à l'action.

De manière générale, les files d'attente constituent une vulnérabilité bien identifiée. Lorsqu'elles se déroulent sur la voie publique, elles exposent les visiteurs ou spectateurs à des attaques dont

le niveau de complexité peut varier énormément (armes blanches, véhicules béliers, armes à feu, explosifs, etc.).

De même, les entrées et sorties de spectacles et de séances de cinéma, ne pouvant être étalées dans le temps doivent donner lieu à une vigilance spécifique aux abords des établissements.

Modes d'action privilégiés

Les attaques à l'**arme blanche** et les risques posés par le recours à des **véhicules béliers** imposent une vigilance particulière compte tenu de la spécificité des lieux culturels (files d'attente, horaires fixes). L'histoire récente démontre que le risque d'attaques plus complexes utilisant des **armes à feu** et des **explosifs** n'est pas à exclure.

Mesures préventives et réactives

Les mesures de prévention situationnelle, la gestion de flux et des files d'attente sont les éléments clés de la prévention de la menace terroriste. Des relations régulières avec les forces de sécurité intérieure permettent une meilleure connaissance de l'établissement et facilitent à terme l'intervention de celles-ci. L'organisation d'événements ponctuels ou récurrents peut impliquer une préparation en amont avec la police et la gendarmerie dans un souci d'efficacité.

Outre les relations avec les forces de sécurité locales, les exploitants d'établissements culturels sont invités à se rapprocher des référents sûreté des groupements de gendarmerie et des directions départementales de la sécurité publique. Au sein du ministère de la Culture, les interlocuteurs sont le service du haut fonctionnaire de défense et de sécurité (SHFDS) et les directeurs adjoints des affaires culturelles en régions ou les directeurs des affaires culturelles en outre-mer, référents sûreté sécurité locaux du ministère.

Liens utiles

Gérer la sûreté et la sécurité des évènements et sites culturels | culture.gouv.fr

Action de renforcement et surveillance des lieux culturels | culture.gouv.fr

SÉCURISATION DES LIEUX DE CULTE

Les menaces et cibles spécifiques

Le niveau de la menace planant les lieux de culte se maintient à un niveau durablement élevé, comme l'ont rappelé l'attaque de la mosquée de Bayonne (2019) ou les attentats de Saint-Étienne-Du-Rouvray (2016) et Nice (2020).

Les trois principales religions monothéistes (christianisme, islamisme et judaïsme) sont particulièrement exposées à un risque d'attaque, notamment en raison de leur prééminence dans la société française et de la farouche opposition idéologique de certains groupes violents.

D'une part, les lieux de culte catholiques et judaïques (chapelles, églises, cathédrales, lieux de pèlerinages, synagogues) sont majoritairement visés par les organisations islamistes sunnites radicales.

D'autre part, les lieux de culte musulmans (mosquées et zaouïa) peuvent être pris pour cibles tant par des organisations terroristes islamistes que par l'extrême droite. Les premières cherchent, là encore, à punir une pratique de l'islam jugée trop légère tandis que les secondes s'inscrivent dans une logique de vengeance et de compensation de précédents attentats islamistes.

Les attaques de lieux de culte sont ainsi un moyen de garantir un retentissement considérable et de cristalliser un certain nombre de tensions sociétales, en attaquant des communautés religieuses structurées.

Les lieux de cultes représentent une cible relativement facile à atteindre pour des individus malveillants pour plusieurs raisons :

- Ils sont généralement accessibles sur de larges plages horaires.
- Les entrées sont peu surveillées et font rarement l'objet de contrôles renforcés, jugés incompatibles avec les activités cultuelles.
- Les bâtiments, souvent anciens, sont peu sécurisés.

- Les célébrations réunissent ponctuellement de nombreux fidèles dans des conditions et à des dates connues de tous.
- Le nombre très élevé de lieux de culte sur le territoire national complexifie leur sécurisation par les pouvoirs publics.

Modes d'action privilégiés

De fait, les attaques à l'**arme blanche** ou aux **armes à feu** sur des fidèles ou les clercs pendant les heures d'ouverture sont le mode opératoire privilégié par les attaquants. La faible sécurisation des lieux de culte offre de grandes chances de succès avec un investissement matériel et opérationnel minimal.

La présence d'un grand nombre de fidèles au moment des prières ou des fêtes religieuses peut également être l'opportunité pour les attaquants de maximiser le nombre de victimes. Une vigilance particulière doit donc être portée sur ces périodes.

A noter que tous les lieux de culte sont susceptibles d'être attaqués : la menace ne saurait être circonscrite aux lieux de cultes majeurs (Lourdes, Grande Mosquée de Paris, etc.).

Mesures préventives et réactives

Cependant, un certain nombre de mesures et de réflexes peuvent limiter considérablement les risques d'occurrence ou les dommages d'une attaque. Ce guide vise ainsi à fournir des éléments pour mieux se préparer et mieux réagir à une attaque, qu'elle soit terroriste ou non. La protection bâtimentaire, les procédures d'alertes et la **formation des acteurs** sont des axes d'améliorations prioritaires : vous trouverez dans ce document des conseils et des outils qui vous aideront à mieux sécuriser votre lieu de culte.

Liens utiles

Protection des lieux à caractère religieux | interieur.gouv.fr

Plan d'action « Sécurité Cathédrales » | culture.gouv.fr

Gérer la sûreté et la sécurité des évènements et sites culturels | culture.gouv.fr

SÉCURISATION DES MAGASINS ET CENTRES COMMERCIAUX

Les menaces et cibles spécifiques

Établissement recevant un public large et varié, les magasins et centres commerciaux peuvent être des cibles d'intérêt (Trèbes en mars 2018). Les recommandations de ce guide visent ainsi à mettre en œuvre des mesures de sûreté compatibles avec l'activité économique et efficaces contre l'ensemble des malveillances : de la petite délinquance (incivilités, agressions, vols) au crime organisé (braquage, acte terroriste).

Dans un contexte de menace durablement élevée, les fortes affluences des fêtes de fin d'année ou les opérations promotionnelles réunissant une population importante dans un lieu clos peuvent constituer une aggravation des conséquences éventuelles d'une attaque (panique, bousculade, nombre de victimes potentielles, etc.)

Les centres commerciaux présentent certaines vulnérabilités inhérentes à leurs activités. Ainsi, la libre circulation du public, le nombre d'accès et l'étendue des infrastructures peuvent être exploitées par des individus malveillants. Les files d'attentes ou les regroupements constituent également une vulnérabilité bien identifiée et exposent le public à des attaques variées (armes blanches, véhicules béliers, armes à feu, explosifs, etc.).

Modes d'action privilégiés

Le recours à des **armes de guerre,** à des **armes blanches** ou à des **véhicules béliers** pourraient être les modes d'action privilégiés pour les attaques de ces établissements. Toutefois, les autres modes opératoires ne doivent pas être exclus, en particulier l'utilisation d'**explosifs**, la **prise d'otage**, l'**attaque chimique** ou même la création de mouvements de panique à l'aide de pétards ou d'incendies.

Mesures préventives et réactives

Les exploitants doivent accorder une attention particulière à ces menaces, notamment par :

- La tenue à jour de leur **plan de sécurisation d'établissement** ;
- La mise en place d'un **plan de vidéo protection** ;
- Le **contrôle de certains accès** ;
- L'organisation d'**exercices de sûreté** ;
- La **formation de leur personnel**, notamment en ce qui concerne l'alerte et la réaction.
- Des échanges d'information devant faciliter l'adaptation de la posture sûreté du centre commercial.

Ce guide vise ainsi à fournir des conseils opérationnels pour mettre en œuvre ces mesures préventives.

Par ailleurs, les directeurs d'établissements sont invités à se rapprocher des forces de sécurité intérieure (notamment via les référents sûreté départementaux) pour affiner l'analyse des menaces et des vulnérabilités. Les fédérations professionnelles peuvent également apporter leur concours par la rédaction d'une documentation spécialisée.

Liens utiles

Magasins drive | economie.gouv.fr

Un troisième niveau pour le plan Vigipirate : quelles incidences dans les entreprises privées et publiques ? - CNPP | cnpp.com

SÉCURISATION DES ADMINISTRATIONS PUBLIQUES ET PRIVÉES

Les menaces et cibles spécifiques

Les administrations publiques et privées sont confrontées à un niveau de malveillance élevé et relativement constant en raison de la diversité des menaces. Définies comme l'ensemble des espaces accueillant du public et fournissant une offre de service, qu'ils dépendent de l'État ou d'un organisme privé, elles incluent les agences bancaires et assurances, les centres des finances, les mairies et préfectures, les conseils départementaux, les CPAM, les locaux politiques et syndicaux, etc.

Ces espaces peuvent être pris pour cibles par plusieurs types d'individus malveillants, aux motivations variables :

- Les usagers devenant violents quand leurs demandes ne sont pas satisfaites ;
- Les mouvements sociaux contestataires qui occupent ou saccagent des locaux de l'État ou d'une entreprise privée ;
- La malveillance interne ;
- Les délinquants et criminels s'intéressant aux espaces dans lesquels sont échangées ou stockées des valeurs, susceptibles de s'appuyer sur la collaboration de quelqu'un de l'intérieur ;
- Les terroristes qui visent des administrations symboliques ou dans lesquels le nombre de victimes potentielles est important.

Modes d'action privilégiés

Les modes d'actions vont des coups à mains nues sur les employés, à l'**usage d'armes blanches ou à feu** (attaque du commissariat de Rambouillet en 2021) ainsi que le recours à des **engins explosifs improvisés** (centre des finances publiques de Bastia en 2019) , voire sont liés à la cybersécurité et au vol de données.

Mesures préventives et réactives

D'une manière générale, les individus malveillants vont en premier lieu chercher à exploiter les points faibles de leurs cibles. Pour les administrations publiques et privées, les vulnérabilités principales résident dans leur nature même : l'accueil du public sur l'ensemble du territoire. Au regard de la nature des menaces et des modes opératoires les plus fréquents, il conviendra donc de porter une attention particulière sur le **contrôle des accès**, la procédure d'alerte et la **formation du personnel** qui peuvent être facilement améliorés et élèveront rapidement la sécurité des lieux. Cependant, ces mesures doivent être adaptées : il faudra concilier la préservation de la sûreté avec l'accueil du public, sans entraver l'activité quotidienne du personnel et des usagers.

Les recommandations de ce guide permettent de limiter l'occurrence ou les effets de l'ensemble de ces menaces, en améliorant le niveau global de sécurité. La plupart des administrations dépendant d'entités plus larges (État ou siège social de l'entreprise), il leur est avant tout demandé de suivre les directives édictées par la hiérarchie et, le cas échéant, la direction sûreté du groupe. Les référents sûreté de la police et de la gendarmerie nationales peuvent également fournir des indications sur le contexte sécuritaire local et émettre des recommandations adaptées à la structure.

Liens utiles

Un troisième niveau pour le plan Vigipirate : quelles incidences dans les entreprises privées et publiques ? - CNPP | cnpp.com

SÉCURISATION DES GRANDS RASSEMBLEMENTS EXTÉRIEURS

Les menaces et cibles spécifiques

La menace planant sur les grands rassemblements extérieurs est durablement élevée et principalement de nature islamiste. En effet, les attaques terroristes de Nice (juillet 2016) ou de Berlin (décembre 2016) illustrent l'intérêt que portent les groupes terroristes pour les évènements réunissant une foule compacte en extérieur. La notion de « grands rassemblements extérieurs » implique la réunion d'un nombre élevé de personnes, de manière relativement dense, en un lieu unique qui peut être un terrain privé tout comme la voie publique. Ainsi, les manifestations sportives et culturelles, les marchés, fêtes populaires, mouvements sociaux ou tout autres évènements de ce type sont concernés par cette fiche.

Ces regroupements sont, la plupart du temps, des moments de festivité ou de célébration. Ils incarnent ainsi le mode de vie occidental et sont donc susceptibles d'être pris pour cibles par des terroristes islamistes. En effet, la propagande djihadiste incite régulièrement à s'en prendre à ce type d'événements symboliques considérés comme contraires aux valeurs de l'islamisme radical. De plus, le nombre élevé de personnes présentes sur les lieux leur permet de maximiser le nombre de victimes sur un court laps de temps. Enfin, la médiatisation de certains de ces rassemblements (festivals, marathon, fête de la musique, etc.) assure un certain retentissement à l'action des assaillants. Pour toutes ces raisons, les grands rassemblements extérieurs sont aujourd'hui des cibles privilégiées par les groupes terroristes. Les recommandations de ce guide permettent donc de réduire ce risque, mais plus généralement de se prémunir contre toute forme de criminalité ou de délinquance.

Modes d'action privilégiés

Les grands rassemblements extérieurs souffrent d'un certain nombre de vulnérabilités. Parmi lesquelles, la difficulté d'effectuer un contrôle systématique des allées et venues. Un effort doit être porté sur la vigilance du personnel et des participants, la chaîne d'alerte ainsi que les réactions à tenir. Dans la mesure du possible et le plus en amont possible, les forces de sécurité intérieure (police ou gendarmerie) doivent être associées à l'organisation *via* les référents sûreté départementaux.

Les dernières attaques sur les lieux de rassemblement en France et à l'étranger ont montré la répétition de certains modes opératoires :

- L'**utilisation d'explosifs :** dissimulés sur une personne, dans un sac ou un véhicule, ils peuvent faire un grand nombre de victimes au milieu de la foule.
- Le recours à une **arme blanche :** difficilement détectable, le nombre de victimes est généralement moins élevé.
- Le recours à des **armes à feu :** un tireur mobile dans l'espace peut faire un grand nombre de victimes.
- L'attaque au **véhicule bélier :** un véhicule est lancé à pleine vitesse sur la foule. Si le nombre de victime peut être élevé, les mesures préventives sont relativement faciles à mettre en place.

Adaptées aux grands rassemblements extérieurs, ce ne sont cependant pas les seules méthodes utilisées par les terroristes.

Mesures préventives et réactives

Les mesures présentées dans ce guide permettent de limiter la probabilité d'une attaque ou de réduire son impact. Concernant les grands rassemblements extérieurs, il est nécessaire de **former le personnel** et de mettre en place des procédures en cas de survenues d'un évènement anormal.

Liens utiles

Guide des bonnes pratiques de sécurisation d'un évènement de voie publique | interieur.gouv.fr

Gérer la sûreté et la sécurité des évènements et sites culturels | culture.gouv.fr

SÉCURISATION DES GRANDS RASSEMBLEMENTS INTÉRIEURS

Les menaces et cibles spécifiques

La menace terroriste qui pèse sur les grands rassemblements en milieux clos est durablement élevée, comme l'ont rappelé les attentats du Bataclan et du Stade de France en novembre 2015. En effet, les concerts, spectacles, rencontres sportives, marchés couverts ou salons professionnels, etc. sont autant de cibles privilégiées par les assaillants.

Ces espaces publics fermés accueillant un public important souffrent de plusieurs vulnérabilités :

- La charge symbolique et la médiatisation des évènements tels que les concerts, spectacles ou matchs sportifs qui incarnent le mode de vie à l'occidental. Les attaquer est un moyen pour les terroristes de signifier leur opposition à la culture occidentale.
- Ils réunissent un grand nombre de personnes qui, en plus d'être une cible facile, peuvent facilement être prises au piège en cas de difficultés d'évacuation.
- L'environnement peut retarder l'alerte : l'organisation et la taille de l'espace, les conditions sonores et lumineuses ou la nature du public peuvent accroître le temps d'alerte, de réaction et l'intervention des forces de l'ordre.

Modes d'action privilégiés

Aujourd'hui, la plupart des organisateurs d'événements ont intégré la présence d'une menace. Ainsi, les entrées sont très souvent filtrées et la sécurité des lieux assurée par une entreprise privée, en lien avec les forces de l'ordre. Bien qu'efficaces, ces mesures ne permettent pas d'exclure totalement le risque. Celui-ci se concentre principalement sur deux modes opératoires.

- D'abord la **fusillade :** un ou plusieurs individus parviennent à pénétrer dans l'enceinte de l'événement et conduisent un périple meurtrier en visant la foule.
- Ensuite, le recours à un **engin explosif improvisé :** placé dans un sac ou sur un individu, il est activé au milieu de la foule.

Bien que d'autres modes opératoires soient fréquemment utilisés par les terroristes, ceux-ci sont adaptés aux grands rassemblements en milieu clos. En effet, ils permettent de toucher un grand nombre de victimes de manière indifférenciée et très rapide.

Mesures préventives et réactives

Ce guide recommande un certain nombre de mesures pour se prémunir de ce type d'attaque mais plus largement contre tous types de malveillance, y compris celles du bas du spectre. Concernant les grands rassemblements en milieu clos, il est nécessaire de mettre en place un **plan de sécurisation de l'établissement** (en lien avec les référents sûreté départementaux de la police et de la gendarmerie), de **former le personnel** et de mettre en place des procédures en cas de survenue d'un évènement anormal.

Liens utiles

Gérer la sûreté et la sécurité des évènements et sites culturels | culture.gouv.fr

Un troisième niveau pour le plan Vigipirate : quelles incidences dans les entreprises privées et publiques ? - CNPP | cnpp.com

SÉCURISATION DES SITES TOURISTIQUES

Les menaces et cibles spécifiques

La menace terroriste pèse sur les sites touristiques de manière durablement élevée comme l'a rappelé l'attentat du 14 juillet 2016 sur la promenade des anglais à Nice, ou encore l'attentat au Carrousel du Louvre le 3 février 2017. En effet, les sites touristiques peuvent faire l'objet d'attaques eu égard à leur forte fréquentation et à leur symbole. Dès lors, ils sont parmi les lieux des plus vulnérables, offrant aux terroristes une gamme de cibles très médiatisées. Aussi, les sites touristiques peuvent être particulièrement à risque, car ils sont souvent un symbole culturel, voire religieux ou politique.

Les sites touristiques présentent certaines vulnérabilités inhérentes à leurs activités. Ainsi, la libre circulation du public, le nombre d'accès et l'étendue des infrastructures peuvent être exploitées par des individus malveillants. De même, les abords de ces établissements constituent également une cible potentielle et exposent le public à des attaques variées. De manière générale, les files d'attente constituent une vulnérabilité bien identifiée. Lorsqu'elles se trouvent sur la voie publique, elles exposent les visiteurs à des attaques dont le niveau de complexité peut varier énormément.

Ces attaques diffèrent sensiblement selon les caractéristiques spécifiques à chaque site en fonction de sa taille, de son emplacement, de sa disposition et de son fonctionnement, toutefois l'utilisation de ce guide doit permettre d'abaisser autant que possible le niveau de la menace terroriste.

Modes d'action privilégiés

Il est possible que vous soyez confrontés à une attaque terroriste lorsque vous vous trouvez dans un lieu touristique. Celle-ci peut alors se caractériser par une **alerte à la bombe**, un **véhicule bélier,** un **engin explosif improvisé,** un **colis suspect** paraissant abandonné aux abords d'un lieu touristique donné, ou encore d'une attaque à l'**arme blanche**. Dans ces scénarios, les touristes pourraient être gravement touchés et le site endommagé ou détruit.

Au-delà de ces attaques « physiques », elles pourraient aussi être **numériques,** directement sur internet par l'entremise de bornes Wi-Fi.

Bien que ces modes opératoires soient fréquemment utilisés par les terroristes, il convient de mettre en œuvre une vigilance globale afin de prévenir toute tentative d'attaque. En effet, il n'est pas impossible que d'autres modes opératoires se développent demain contre les sites touristiques.

Les mesures mises en place contribuent ainsi à élever le niveau global de sécurité et plus généralement à se prémunir contre toute forme de criminalité ou de délinquance.

Mesures préventives et réactives

L'environnement d'un site touristique doit être sûr et sécurisé. Pour parvenir à cette fin, il est essentiel que la sécurisation du site soit entreprise de concert avec les forces de sécurité intérieure.

Les mesures de prévention situationnelle, la gestion de flux et des files d'attente sont les éléments clefs de la prévention de la menace terroriste. De même, des procédures internes de confinement ou d'évacuation doivent permettre une gestion rapide et efficace du public et du personnel situé dans l'enceinte d'un site face à une attaque directe, ou lors d'une attaque à proximité. Des relations régulières avec les forces de sécurité intérieure permettent une meilleure connaissance du site et facilitent à terme l'intervention de celles-ci. L'organisation d'événements ponctuels ou récurrents peut impliquer une préparation en amont avec la police et la gendarmerie dans un souci d'efficacité.

Outre les relations avec les forces de sécurité locales, les exploitants de sites touristiques sont invités à se rapprocher des référents sûreté des groupements de gendarmerie et des directions départementales de la sécurité publique. Au sein du ministère de l'Économie et des Finances, comme au sein du ministère de la Culture, l'interlocuteur est le service du haut fonctionnaire de défense et de sécurité (SHFDS).

Liens utiles

Gérer la sûreté et la sécurité des évènements et sites culturels | culture.gouv.fr

Un troisième niveau pour le plan Vigipirate : quelles incidences dans les entreprises privées et publiques ? - CNPP | cnpp.com

SÉCURISATION DES HÔTELS ET RESTAURANTS

Les menaces et cibles spécifiques

La menace terroriste pèse sur les établissements hôteliers et les restaurants de manière durablement élevée comme l'ont rappelé les attentats du 13 novembre 2015 place de la République à Paris. En effet, les établissements hôteliers et les restaurants peuvent faire l'objet d'attaques eu égard au public qu'ils accueillent et au symbole qu'il représente.

Les hôtels et restaurants présentent certaines vulnérabilités inhérentes à leurs activités. Ainsi, la libre circulation du public, le nombre d'accès et l'étendue des infrastructures peuvent être exploitées par des individus malveillants. De même, les abords de ces établissements constituent également une vulnérabilité et exposent le public à des attaques variées.

Les périodes de vacances scolaires ou les pics d'activité touristique sont autant de moments qui augmentent le risque de réalisation des diverses menaces (incivilités, agressions, acte terroriste, etc.) compte tenu des rassemblements importants de population.

Ces attaques diffèrent sensiblement en fonction des caractéristiques spécifiques à chaque établissement, qu'il s'agisse d'hôtels ou de restaurants. En effet, même si chaque établissement est spécifique en fonction de sa taille, de son emplacement, de sa disposition et de son fonctionnement, l'utilisation de ce guide doit permettre d'abaisser autant que possible la probabilité de survenue ou les conséquences d'une attaque terroriste..

Modes d'action privilégiés

Il est possible que votre établissement hôtelier ou restaurant devienne la cible d'une attaque terroriste. Celle-ci peut alors se caractériser par une **alerte à la bombe,** un **engin explosif improvisé,** une **attaque chimique,** un **véhicule bélier,** un **colis suspect** paraissant abandonné aux abords de l'établissement, la création de mouvements de panique à l'aide de pétards ou d'incendies, ou encore une attaque à l'**arme** comme ce fut le cas lors de l'attentat terroriste de Paris du 12 mai 2018. Dans ces scénarios, le personnel ainsi que la clientèle pourraient être gravement touchés et les locaux pourraient être endommagés ou détruits.

Au-delà de ces attaques « physiques », elles pourraient aussi être **numériques,** directement sur internet ou par l'entremise d'un **extérieur.**

Bien que ces modes opératoires soient fréquemment utilisés par les terroristes, il convient de mettre en œuvre une vigilance globale afin de prévenir toute tentative d'attaque. En effet, il n'est pas impossible que d'autres modes opératoires se développent demain contre les établissements hôteliers et restaurants.

Les mesures mises en place contribuent ainsi à élever le niveau global de sécurité et plus généralement à se prémunir contre toute forme de criminalité ou de délinquance.

Mesures préventives et réactives

L'environnement qui entoure un hôtel ou un restaurant doit être sûr et sécurisé. Pour parvenir à cette fin, il est essentiel que la sécurisation de cet établissement soit entreprise de concert avec les forces de sécurité intérieure afin de parfaire cette vigilance.

La mise en œuvre de mesures préventives est essentielle en ce qu'elle permettra également de lutter contre d'autres formes de criminalités au sein de l'établissement, comme le vol, le cambriolage et l'incendie criminel.

Pour parvenir à cet équilibre, plusieurs mesures peuvent être mise en œuvre dans le cadre du plan de sécurisation de l'établissement (PSE) :

- Assurer des partenariats en fonction des contextes locaux, en particulier avec les forces de sécurité ;
- Mettre en place un plan de **vidéo protection** ;
- Élaborer des consignes et des protocoles d'information des agents et du public ;
- Préparer un plan de crise ;
- Scénariser et planifier les **exercices de simulation** ;
- S'assurer que les procédures retenues sont connues et maîtrisées par le personnel concerné en mettant en place des **formations** régulières ;
- Ne pas minorer le risque attentat quel que soit le lieu d'implantation de l'établissement ;
- Adapter les réactions en cas d'attaque : l'évacuation d'urgence n'est pas nécessairement la solution la meilleure. Le confinement peut être préféré en cas d'attaque extérieure ;

- En cas d'intervention des forces de sécurité, suivre leurs consignes de façon prioritaire. Il est important que les équipes de direction adoptent une démarche permanente de sécurité.

Liens utiles

La filière restauration | entreprises.gouv.fr

Hôtellerie : hôtels de tourisme et auberges collectives | entreprises.gouv.fr

Hôtels et restaurants | economie.gouv.fr

Un troisième niveau pour le plan Vigipirate : quelles incidences dans les entreprises privées et publiques ? - CNPP | cnpp.com

SÉCURISATION DES LIEUX DE VIE NOCTURNE

Les menaces et cibles spécifiques

La menace terroriste pèse sur les établissements de vie nocturne de manière durablement élevée comme l'ont rappelé les attentats du 13 novembre 2015 au Bataclan à Paris. En effet, les établissements de vie nocturne peuvent faire l'objet d'attaques eu égard au public qu'ils accueillent et au symbole qu'il représente..

Les établissements de vie nocturne présentent certaines vulnérabilités inhérentes à leurs activités. Ainsi, la libre circulation du public, le nombre d'accès et l'étendue des infrastructures peuvent être exploitées par des individus malveillants. La consommation d'alcool ou de produits stupéfiants aux abords de ces établissements constituent en outre une baisse de vigilance propice à la surprise.

En effet, même si chaque établissement est spécifique en fonction de sa taille, de son emplacement, de sa disposition et de son fonctionnement, l'utilisation de ce guide doit permettre d'abaisser autant que possible la probabilité ou les conséquences d'une attaque terroriste..

Modes d'action privilégiés

Il est possible que votre bar, club ou casino devienne la cible d'une attaque terroriste. Elle peut prendre la forme d'une **alerte à la bombe,** un **engin explosif improvisé,** une **attaque chimique,** un **véhicule bélier,** un **colis suspect** paraissant abandonné aux abords de l'établissement, la création de mouvements de panique à l'aide de pétards ou d'incendies, ou encore d'une attaque à l'**arme blanche.** Dans ces scénarios, le personnel ainsi que la clientèle pourraient être gravement touchés et les locaux pourraient être endommagés ou détruits.

Au-delà de ces attaques « physiques », elles pourraient aussi être **numériques,** directement sur internet ou par l'entremise d'un **extérieur.**

Bien que ces modes opératoires soient fréquemment utilisés par les terroristes, il convient de mettre en œuvre une vigilance globale afin de prévenir toute tentative d'attaque. En effet, il n'est pas impossible que d'autres modes opératoires se développent demain contre les établissements de vie nocturne.

Les mesures mises en place contribuent ainsi à élever le niveau global de sécurité et plus généralement à se prémunir contre toute forme de criminalité ou de délinquance.

Mesures préventives et réactives

L'environnement qui entoure un établissement de vie nocturne doit être sûr et sécurisé. Pour parvenir à cette fin, il est essentiel que la sécurisation de cet établissement soit entreprise de concert avec les forces de sécurité intérieure.

La mise en œuvre de mesures préventives est essentielle en ce qu'elle permettra également de lutter contre d'autres formes de criminalités au sein de l'établissement, comme le vol, le cambriolage ou l'incendie criminel.

Plusieurs mesures peuvent être mise en œuvre dans le cadre du **Plan de Sécurisation de l'Établissement** (PSE) :

- Assurer des partenariats en fonction des contextes locaux, en particulier avec les forces de sécurité intérieure ;
- Mettre en place un plan de **vidéo protection** ;
- Élaborer des consignes et des protocoles d'information des agents et du public ;
- Préparer un **plan de crise** ;
- Scénariser et planifier les **exercices de simulation** ;
- S'assurer que les procédures retenues sont connues et maîtrisées par le personnel concerné en mettant en place des **formations** régulières ;
- Ne pas minorer le risque attentat quel que soit le lieu d'implantation de l'établissement ;
- Adapter les réactions en cas d'attaque : l'évacuation d'urgence n'est pas nécessairement la solution la meilleure. Le confinement peut être préféré en cas d'attaque extérieure ;
- En cas d'intervention des forces de sécurité, suivre strictement leurs consignes. Il est important que les équipes de direction adoptent une démarche permanente de sécurité.

Liens utiles

Vie Nocturne | Plateforme de la Vie Nocturne

Monde de la nuit | umih.fr

Un troisième niveau pour le plan Vigipirate : quelles incidences dans les entreprises privées et publiques ? - CNPP | cnpp.com

SÉCURISATION DES ÉCOLES ET DES ÉTABLISSEMENTS SCOLAIRES

Les menaces et cibles spécifiques

Les écoles et établissements scolaires constituent des cibles d'attaques (physiques ou informatiques). Le nombre important d'élèves et de personnels accueillis, la configuration des locaux plus ou moins ouverts ainsi que la charge symbolique que sont les lieux de construction du savoir et de partage de la connaissance sont autant de vulnérabilités identifiées. L'attentat du vendredi 16 octobre 2020 à Conflans-Sainte-Honorine à l'encontre d'un professeur, mais également les fusillades et tueries de masse perpétrées au sein des établissements scolaires de pays étrangers rappellent le caractère très sensible de ces derniers.

Ces menaces, qui sont par nature évolutives, sont susceptibles d'avoir un caractère terroriste. La menace terroriste islamiste pèse en effet sur « l'enseignement » de façon indistincte et donc aussi sur les établissements scolaires.

Par ailleurs, ces attaques diffèrent sensiblement en fonction des caractéristiques spécifiques de chaque établissement notamment en fonction de leur taille, leur emplacement, leur disposition ainsi que leur fonctionnement.

Modes d'action privilégiés

Les modes d'actions se caractérisent par une grande diversité de moyens utilisés tels que :

- une **alerte à la bombe**, un **engin explosif improvisé** ou encore un **colis suspect** paraissant abandonné au sein ou aux abords de l'établissement ;
- une **attaque physique** par l'utilisation d'une arme blanche, comme ce fut le cas lors de l'attentat terroriste du 16 octobre 2020 ;
- une attaque avec une arme par destination (type attaque par un **véhicule bélier**) ;
- une **attaque des systèmes d'informations**.

Les modes opératoires précédemment évoqués ne sont pas exhaustifs. L'objectif est donc de se préparer au mieux à répondre à tout type de menace visant les établissements d'enseignement et la communauté éducative.

Mesures préventives et réactives

Les mesures mises en œuvre dans le cadre de la sécurisation des établissements scolaires face à la menace attentat-intrusion concourent également à la lutte contre d'autres formes potentielles d'atteintes aux biens ou aux personnes. La sécurisation doit donc être pensée globalement pour en assurer la cohérence.

D'une part, la sécurisation des établissements ne peut s'opérer sans une approche partenariale entre :

- les acteurs du service de l'éducation : le directeur d'école ou chef d'établissement, les équipes mobiles de sécurité académiques, les référents sûreté éducation nationale, les référents radicalisation, les responsables de la sécurité des systèmes d'information ;
- et les partenaires extérieurs du service de l'éducation, à savoir les forces de sécurité intérieure, la préfecture de département et les collectivités territoriales gestionnaires.

Cela se traduit notamment par le partage de coordonnées, d'informations et de bonnes pratiques, par l'accompagnement des établissements dans la mise en œuvre des mesures de sécurisation, en lien avec les correspondants « sécurité-école » identifiés parmi les forces de sécurité intérieure ou encore par des actions de **formation** conduites en partenariat avec le ministère de l'intérieur[3].

Par ailleurs, les écoles et établissements scolaires sont soumis à un dispositif de sécurisation face à la menace attentat intrusion[4] qui les assujettit à :

- l'élaboration d'un plan particulier de mise en sûreté « attentat-intrusion » ;
- la réalisation annuelle d'un **exercice** « attentat-intrusion » ;

3 Un protocole de partenariat portant sur la formation à la prévention et à la gestion de crise a notamment été signé par le ministère chargée de l'éducation nationale et la gendarmerie nationale.

4 Ces mesures sont détaillées par l'instruction INTK1711450J du 12 avril 2017 relative au renforcement des mesures de sécurité et de gestion de crise applicables dans les écoles et les établissements scolaires.
Les responsables des structures d'accueil collectif de mineurs à caractère éducatif, des centres accueillant des séjours SNU et des établissements publics de sport pourront s'inspirer de ces mesures pour la sécurisation de leur établissement.

- la dotation d'un système d'alerte et d'une chaine de remontées ;
- la mise à disposition des plans des bâtiments aux partenaires ;
- l'appropriation des comportements réflexes par la communauté éducative via des actions de **sensibilisation et de formation** ;
- un contrôle visuel des sacs, un contrôle des flux ainsi que la **vérification systématique des identités des personnes étrangères à l'établissement**, consignes émanant du plan gouvernemental de vigilance, de prévention et de protection « Vigipirate ».

Pour compléter ce dispositif de sécurisation, il est également fortement recommandé que soit élaboré, avec le concours des forces de sécurité intérieure, un diagnostic de mise en sûreté, préalable jugé nécessaire eu égard à l'état de la menace pesant sur les écoles et établissements scolaires.

En outre, une attention particulière doit être portée aux abords de l'établissement en évitant tout attroupement préjudiciable à la sécurité des élèves et des personnels ainsi qu'aux activités périscolaires et aux manifestations recevant du public lors des fêtes de fin d'année scolaire, kermesses et autres événements. Les organisateurs de manifestations ou d'événements particuliers doivent coordonner leurs actions avec les services préfectoraux afin de déterminer les mesures de sécurisation à mettre en œuvre en fonction du contexte local.

Enfin, les directeurs d'école et chefs d'établissement pourront s'appuyer sur les autorités académiques en lien avec le service du haut fonctionnaire de défense et de sécurité du ministère chargé de l'éducation nationale, en complément des fiches thématiques et conduites à tenir proposées dans ce guide, qui visent à apporter une aide opérationnelle en cas d'événement grave.

SÉCURISATION DES ÉTABLISSEMENTS D'ENSEIGNEMENT SUPÉRIEUR ET DE RECHERCHE

Les menaces et cibles spécifiques

Les établissements d'enseignement supérieur et de recherche (universités, écoles et organismes de recherche), ci-après « les établissements », constituent des cibles potentielles d'attaques (physiques ou informatiques) notamment du fait du nombre important de leurs usagers et personnels ainsi qu'à titre symbolique, en tant que lieux de construction du savoir et de partage de la connaissance. De plus, les campus ouverts des établissements et la structure de leurs locaux (nombreux amphithéâtres etc.) constituent des sources de vulnérabilités potentielles.

Les activités de recherche des établissements sont également, en tant que telles, la cible potentielle d'attaques ayant des motivations économiques et/ou géostratégiques. Elles sont exposées à des risques de captation, d'ingérence étrangère et autres menaces pesant sur le potentiel scientifique et technique de la nation : risques d'atteinte aux intérêts économiques de la nation ; d'atteinte aux capacités nationales de défense et de renforcement des arsenaux militaires étrangers (biens à double usage) ; risque de contribution à la prolifération des armes de destruction massive et de leurs vecteurs ; ou encore de favoriser des actes terroristes sur le territoire national ou à l'étranger.

Toutes ces menaces, qui sont par nature évolutives, sont susceptibles d'avoir un caractère terroriste. La menace terroriste islamiste pèse en effet sur « l'enseignement » de façon indistincte et donc aussi sur les établissements d'enseignement supérieur et de recherche.

Modes d'action privilégiés

Les menaces pesant sur ces établissements sont plurielles : **intrusions**, attaques contre des personnes (usagers ou personnels), dégradations matérielles, vols de données ou de matériels, etc. Les attaques physiques potentielles peuvent s'accompagner de l'usage de moyens très divers : engins explosifs (**improvisé** ou **non**) ; **armes** (blanche, à feu, par destination) ; attaque par **véhicule bélier** ; **colis abandonné** au sein ou aux abords de l'établissement, etc. Les établissements d'enseignement supérieur et de recherche peuvent aussi être la cible d'**attaque des systèmes d'informations** : rançongiciels, attaques en déni de service, etc.

Mesures préventives et réactives

La sécurisation des établissements ne peut s'opérer sans une approche partenariale entre différents acteurs, dont le chef d'établissement, le fonctionnaire de sécurité de défense (FSD), le référent radicalisation, le responsable de la sécurité des systèmes d'information (SSI) et autres acteurs de la chaîne fonctionnelle de SSI, ainsi que les partenaires extérieurs. Des conventions entre administrations centrales ministérielles participent à la sécurisation des sites, en particulier avec la délégation ministérielle aux partenariats, aux stratégies et aux innovations de sécurité (DPSIS) du ministère de l'intérieur ainsi qu'avec les directions opérationnelles (PN, GN, PP).

Localement, la sûreté de l'établissement repose très largement sur des interactions nourries de l'établissement avec les forces de sécurité intérieure, les services préfectoraux et de renseignement.

Par ailleurs, des mesures préventives jugées appropriées et efficaces doivent être appliquées. Ces mesures requièrent la prise en compte des caractéristiques spécifiques des établissements. Elles s'appuient notamment sur la prévention technique de la malveillance, ou prévention situationnelle[5]. Ces mesures sont également pertinentes pour lutter contre d'autres formes potentielles d'atteintes aux biens ou aux personnes.

La mise en œuvre de la prévention technique de la malveillance s'inscrit notamment dans un cadre partenarial entre le MESRI et le ministère de l'intérieur. Des référents sûreté (relevant de la DGGNN et de la DGPN) sont déployés dans l'ensemble des départements, en métropole et en outre-mer, appuyés localement par des correspondants sûreté. Il appartient à l'établissement de saisir son référent sûreté en vue d'interventions de différents niveaux parmi lesquels :

- consultation de sûreté ;
- diagnostic de sûreté : document écrit sommaire au profit d'un demandeur présentant un intérêt opérationnel au regard d'un risque particulier auquel il est exposé ;
- audit de sûreté : étude approfondie d'un bâtiment, d'un site, ou de l'établissement dans son ensemble suivie de préconisations techniques, humaines et organisationnelles.

Outre la réalisation d'un audit de sûreté, des dispositions obligatoires dans le périmètre de l'enseignement scolaire et rappelées dans la fiche relative aux écoles et établissements scolaires de ce guide sont pertinentes dans une démarche de sécurisation des établissements d'enseignement supérieur et de recherche.

La conduite d'une opération de sécurisation d'un site suppose la connaissance précise, de sa topographie. Il convient donc que l'établissement facilite les conditions d'intervention des forces de

5 Loi n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure.

sécurité intérieure ce qui implique des contacts privilégiés avec les FSI, la tenue à jour de plans de masse et leur communication aux FSI[6], etc.

Les établissements peuvent également s'appuyer sur le dispositif de protection du potentiel scientifique et technique de la nation (PPST), piloté par le SGDSN[7], visant à protéger les savoirs, savoir-faire et technologies les plus sensibles des établissements publics et privés localisés sur le territoire national. Il se traduit notamment par le contrôle d'accès physique et logique de certaines zones, « zones à régime restrictif » (ZRR).

La sécurisation des unités de recherche sensibles par des ZRR constitue un moyen de lutter contre les captations étrangères et les risques de mésusage de technologies, y compris à des fins terroristes. Cette possibilité est effectuée de façon non ostentatoire et *erga omnes*. Le SDS du MENJ/MESRI, est en charge du suivi de la réglementation PPST pour les établissements de l'ESR.

Focus sur la protection des activités de recherche associée au dispositif de PPST

Le dispositif permet ce qui suit :

- être protégé juridiquement contre les actes malveillants ayant des conséquences sur la compétitivité de l'entité (utilisation frauduleuse d'informations, vol ou captation de données sensibles, pratiques anti-concurrentielles, intrusion dans les systèmes d'information, etc.) ;
- constituer une équipe de travail de confiance ;
- bénéficier d'un accompagnement étatique dans une démarche d'élévation du niveau de sécurité de l'entité ;
- appartenir à une communauté de confiance favorable aux partenariats industriels ;
- flexibilité du dispositif pour l'entité qui identifie et cible son besoin de protection en lien avec le ministère concerné ;
- protection juridique renforcée contre les actes malveillants ayant des conséquences sur la compétitivité de l'établissement ;
- fondement juridique permettant de demander des avis sur les personnes pénétrant dans la ZRR et des sanctions renforcées en cas d'intrusion ou de diffusion des informations protégées.

Enfin, les chefs d'établissement pourront s'appuyer sur les **fiches procédurales** et conduites à tenir proposées dans ce guide, qui vise à apporter une aide opérationnelle en cas d'événement grave.

Liens utiles

Consignes de sécurité établissements scolaires | education.gouv.fr

Sécurité des écoles | education.gouv.fr

6 Mise à disposition en général en préfecture.

7 Le dispositif est fondé sur l'article 413-7 du code pénal et s'organise principalement autour de trois textes d'application : le décret n° 2011-1425 du 2 novembre 2011 ; l'arrêté du Premier ministre du 3 juillet 2012 ; une circulaire interministérielle du 7 novembre 2012.

III. FICHES PROCÉDURALES

SOMMAIRE DES FICHES PROCÉDURALES

Organisation et anticipation (OA) - page 45

OA1 Mise en place d'un plan de sécurisation de l'établissement (PSE). 46
OA2 Formation et sensibilisation du personnel. 49
OA3 Organisation d'un exercice de sûreté . . . 50
OA4 Chaîne d'alerte face à une menace 62
OA5 Vérification du personnel 65
OA6 Préparer sa communication de crise . . . 70
OA7 Conseils aux voyageurs 75

Réaction (R) - page 78

R1 Réaction | Prévenir les autorités 79
R2 Réaction | Attaques armées 81
R3 Réaction | Prise d'otages 85
R4 Réaction | Produits toxiques 86
R5 Réaction | Drones malveillants. 90
R6 Réaction | Cyberattaque 92
R7 Réaction | Signalement d'un individu suspect. 94
R8 Réaction | Fouille des locaux. 99

Moyens (M) - page 100

M1 Moyens | Mise en place d'un système de vidéosurveillance. 101
M2 Moyens | Mise en place d'un système de contrôle des accès. 107
M3 Moyens | Mesures d'entraves aux véhicules béliers 110
M4 Moyens | Mise à niveau de la sécurité des systèmes d'informations. . .112

ORGANISATION ET ANTICIPATION

OA1 | Mise en place d'un plan de sécurisation de l'établissement (PSE). 46
OA2 | Formation et sensibilisation du personnel . 49
OA3 | Organisation d'un exercice de sûreté. . . . 50
OA4 | Chaîne d'alerte face à une menace. 62
OA5 | Vérification du personnel 65
OA6 | Préparer sa communication de crise 70
OA7 | Conseils aux voyageurs 75

FICHE PROCÉDURALE

OA1

MISE EN PLACE D'UN PLAN DE SÉCURISATION DE L'ÉTABLISSEMENT (PSE)

Le plan de sécurisation d'établissement (PSE) définit la politique et l'organisation globale pour sécuriser un établissement. Conçu comme un véritable document structurant pour la sécurité et la sûreté de l'établissement, le PSE se veut un document pratique et doit permettre ainsi à la direction de s'interroger sur des scénarios (tant quotidiens qu'exceptionnels) et d'élaborer des réponses adaptées à la nature des activités et de l'environnement.

La réponse à ces scénarios peut conduire à repenser certains dispositifs : qu'ils soient humains, organisationnels ou techniques. Le PSE constitue le document cadre matérialisant l'engagement de la direction de l'établissement de santé à mener une politique de sécurisation de l'établissement et du personnel.

Ce document est le prolongement du travail d'analyse de risques d'actes de malveillance et de terrorisme et définit les priorités de la politique de sûreté. Le PSE doit faire sens au regard des enjeux de l'établissement et des ressources qu'il peut y consacrer. Dans ce cadre, l'analyse de risque doit tenir compte de l'appréciation des impacts, de l'analyse des vulnérabilités propres à l'établissement et de la probabilité de survenue d'événements malveillants. Il convient d'associer en amont les institutions représentatives du personnel au regard des enjeux portant sur la sécurité et les conditions de travail, a minima sur certains travaux préparatoires du PSE. Toutefois, il est nécessaire de veiller à ne pas diffuser des informations sensibles. À cette fin, l'accès au PSE finalisé devra être limité : en interne à l'établissement, aux seules personnes ayant besoin d'en connaître ; en externe, uniquement auprès des préfectures et des correspondants des FSI. Le PSE portera une mention « diffusion limitée ». Toute publication est formellement à proscrire sur internet ou sur un intranet ne permettant pas une discrimination individuelle des accès. Il est important d'élaborer ce PSE en coordination avec les autorités préfectorales et les forces de sécurité intérieure, ces dernières pouvant apporter leur concours à l'élaboration du plan.

CHECKLIST

Vous trouverez ci-dessous, un plan type de PSE afin de vous aider dans l'organisation et la rédaction de ce dernier.

Préambule – Présentation globale de l'établissement

Bref rapport de présentation de la localisation de l'établissement et de ses activités

Positionnement sur une carte

Chapitre I – Analyse des risques

Description de l'environnement et des particularités de l'établissement

- Environnement et fonctionnement de l'établissement
- Caractéristiques principales de l'établissement
- Organisation fonctionnelle de l'établissement

Risques malveillants pour l'établissement

- Identification des risques
- Hiérarchisation des risques

Vulnérabilités spécifiques de l'établissement

- Identification des points névralgiques
- Hiérarchisation des vulnérabilités

Chapitre II – Sécurisation de l'établissement en temps normal

Mesures de prévention

- Formation, sensibilisation et communication (personnels, sous-traitants, visiteurs, fournisseurs)
- Procédures
- Surveillance

Mesures de protection

- Dispositifs de sûreté en place ou prévus
- Zonages, clôtures et obstacles retardateurs
- Protection des bâtiments, des accès, des parkings
- Contrôle des entrées et des sorties de personnes et de véhicules (personnels, sous-traitants, visiteurs, fournisseurs)
- Dispositif de détection d'intrusion
- Eclairage
- Energie

CHECKLIST

- PC de sécurité
- Protection des systèmes d'informations
- Protection des systèmes de sécurité-sûreté
- Alerte
- Les systèmes internes à l'établissement
- Consignes en cas d'alerte
- Systèmes d'astreinte et de permanence
- Systèmes externes à l'établissement
- Dispositions concernant le personnel et consignes de sûreté
- Procédures de recrutement et d'accès des personnes
- Relation avec les sous-traitants
- Éventuelles équipes de protection et de gardiennage
- Rôle éventuel du personnel des autres branches de la sécurité
- Tests et maintenance périodique du matériel et du personnel de protection

Chapitre III – Sécurisation complémentaire en situation d'attentat ou de crise locale

Alerte, communication et information

- Dossier d'intervention
- Schémas d'alerte

Renforcement de la sécurisation périmétrique et des accès

- Mesures graduelles pouvant être mises en œuvre

Chapitre IV – Maintien en conditions opérationnelles du PSE et articulation avec les autres plans

Exercices

- Organisation retenue pour les exercices de mise en œuvre du PSE

Mise à jour du PSE et des procédures

- Date de la dernière version du PSE et prochaine date de mise à jour

Articulation avec les autres dispositions de l'entreprise

- Plan de continuité d'activité

Liens utiles

Guide d'aide à l'élaboration d'un PSE | solidarites-sante.gouv

FICHE PROCÉDURALE

OA2

FORMATION ET SENSIBILISATION DU PERSONNEL

Le contexte sécuritaire actuel nécessite de former et de sensibiliser l'ensemble des acteurs intervenants sur les espaces publics. En effet, si les conduites à tenir en cas d'attaque de haute intensité sont bien ancrées dans la population, il en est autrement des conduites à tenir par le personnel.

Il est fortement conseillé de sensibiliser l'ensemble de votre personnel aux menaces planant sur votre établissement et de le former sur les procédures à suivre en cas d'acte malveillant. En effet, penser la sécurisation de votre établissement face aux violences qui s'exerceront sur votre personnel ou face aux risques d'attentats ou de sur-attentats, nécessite une approche globale. L'objectif n'est pas de garantir un haut niveau de technicité mais d'assurer une formation continue, régulière, pratique et efficace des agents conformément à votre **PSE** (Plan de sécurisation des établissements) .

Pour ce faire, l'exploitant peut compter sur deux outils :

- **La formation interne :** les procédures sont expliquées à l'ensemble des agents concernés, puis testées lors d'exercice (réels ou sur table) de manière régulière. Un retour d'expérience est organisé afin d'identifier les faiblesses et d'adapter les consignes si nécessaire.
- **La formation externe :** l'exploitant peut demander l'intervention de professionnels externes à son établissement (sociétés de formation, forces de sécurité intérieure, référents sûreté, etc.) afin d'assurer une formation complète et adaptée à l'espace public. Les fédérations professionnelles peuvent vous apporter une expertise dans ce domaine.

Par ailleurs, un certain nombre de ressources sont librement accessibles sur internet. Les **services des hauts fonctionnaires de défense et de sécurité** des différents ministères produisent régulièrement des documents opérationnels et adaptés à votre secteur d'activité. De plus, il existe des MOOC qui délivrent une attestation de suivi que l'employeur peut demander. C'est notamment le cas du MOOC Vigipirate et du MOOC Se former à la sécurité du numérique.

La formation du personnel est un élément clé dans la capacité des espaces publics à faire face à l'ensemble des menaces, de la petite délinquance à l'attentat terroriste. Il convient donc d'y accorder une attention toute particulière et d'y dédier les moyens adaptés.

Liens utiles

Formation à la vigilance, la prévention et la protection face à la menace terroriste - MOOC | SGDSN vigipirate.gouv.fr

Formation à la sécurité du numérique – MOOC | ANSSI secnuacademie.gouv.fr

Plan VIGIPIRATE | sgdsn.gouv.fr

Se former aux premiers secours | gouvernement.fr

FICHE PROCÉDURALE

OA3

ORGANISATION D'UN EXERCICE DE SÛRETÉ

Planifier des exercices

I. Un programme évolutif

La planification d'exercices peut donner lieu à l'élaboration d'une démarche progressive permettant d'augmenter la complexité au fil du temps. Il est possible de commencer par des exercices simples vérifiant l'acquisition de savoirs et la maîtrise des fiches-réflexes. Progressivement, les exercices peuvent gagner en complexité et intégrer des parties de plus en plus grandes de la chaîne de réaction (internes et externes).

Cette montée en gamme n'exonère pas d'évaluations régulières de la mise en œuvre des fiches réflexes pour tenir compte du renouvellement du personnel et de la nécessité d'organiser régulièrement des exercices de différents niveaux de complexité.

L'implication de parties prenantes extérieures (forces de sécurité intérieure, services de secours, etc.) doit se faire sous l'autorité du préfet de département ou, à Paris, du préfet de police.

II. Les différents types d'exercice

Les exercices peuvent être de deux sortes : sur table ou sur le terrain. Quelle que soit la forme retenue, les organisateurs d'exercices peuvent s'appuyer sur les différentes étapes détaillées ci-après.

A. Exercice sur table ou de terrain ?

1. Distinction

L'exercice sur table, exercice cadre ou exercice d'état-major permet de valider des procédures et d'observer la circulation des flux d'information. Il ne permet pas à l'ensemble de la chaîne de s'approprier lesdites procédures. Il présente un intérêt néanmoins pour l'implication des échelons hiérarchiques supérieurs.

L'exercice de terrain est plus approprié pour tester les délais de mise en œuvre des moyens sur le terrain. Il permet aux différents acteurs de s'entraîner et de mettre en œuvre les fiches réflexes évoquées précédemment.

2. Critères de décision

Loin de se limiter à une différence de niveau hiérarchique, la distinction entre les deux types d'exercice peut dépendre des objectifs visés, du thème choisi, des acteurs impliqués, du budget alloué, des délais de réalisation d'un exercice, et enfin de sa durée.

B. Exercices annoncés ou inopinés ?

Encore une fois, les deux possibilités sont offertes et présentent des intérêts différents selon les situations et selon ce qui doit être évalué.

Les exercices inopinés supposent que les joueurs disposent déjà d'une certaine maîtrise du sujet et présentent une difficulté supplémentaire. Ils peuvent être mis en place pour répéter des tâches simples découlant de fiches réflexes.

C. En présence du public ?

D'une manière générale, la présence du public représente un degré supplémentaire de difficulté dont on peut s'affranchir en particulier dans un ERP.

Il est possible, par exemple, de retenir un jour de fermeture ou de décaler l'ouverture un matin le temps de la réalisation de l'exercice. Cette option permet au personnel de participer à l'exercice sur son temps de travail.

Dans certaines circonstances précises, il peut être admis que des exercices se déroulent en présence du public. En dehors des ERP classiques, on peut penser aux d'établissements régis par le code du travail ou aux établissements d'enseignement. En effet, la participation des élèves ou des salariés (pour les immeubles de bureaux) est essentielle et peut apporter une vraie valeur ajoutée dans la prévention puis, le cas échéant, dans la gestion des crises.

Pour les autres catégories d'établissements, il est possible de recourir à des figurants (désignés sous le terme de plastrons) dans le cadre d'un exercice mené sous l'égide des services préfectoraux.

III. Déterminer les objectifs

La méthodologie recommande la déclinaison en objectif général, objectifs intermédiaires et objectifs spécifiques.

A. L'objectif général :

Un objectif général décrit la situation qui existera en fin d'action. Il se décline ensuite en objectifs intermédiaires et spécifiques.

B. Les objectifs intermédiaires :

Ils se définissent comme les actions communes à mener pour atteindre l'objectif général. Le nombre d'objectifs intermédiaires n'est pas limité. Cependant, s'ils sont trop nombreux, il est préférable de réaliser des exercices partiels pour éviter une évaluation trop complexe.

C. Les objectifs spécifiques :

ils s'appliquent à l'ensemble des situations susceptibles de survenir et/ou aux rôles à tenir par les différents participants. Ils peuvent soit être limités dans le temps ou dans l'espace, soit concerner un aspect jugé spécialement intéressant par des joueurs relevant d'organisations différentes.

Objectif principal	Tester les procédures en cas d'attaque terroriste			
Objectifs secondaires	Tester la diffusion de l'alerte			
Objectifs spécifiques	Vérifier les communications avec les forces de l'ordre			

IV. Identifier les acteurs

L'organisation de l'exercice suppose la détermination des grands types de rôle (tant dans la phase de planification que dans la phase de jeu).

A. La direction de l'exercice (DIREX)

Le DIREX est le pilote de l'exercice. Il assume la responsabilité de l'exercice depuis la préparation jusqu'à la synthèse. Il a pour mission :

Avant l'exercice :

- De présider les réunions de lancement, de validation, de finalisation et du Comité de pilotage ;
- De définir les grandes orientations du scénario, en fonction du thème et des objectifs ;
- D'arrêter les conventions d'exercice et les points à observer et évaluer ;
- De se tenir informé de l'état d'avancement de la préparation ;
- D'assurer la communication sur l'exercice (cf. infra) ;
- De valider le dossier d'exercice et le dossier « joueur » ;
- D'entériner toute mesure relative à la logistique.

Pendant :

- D'assurer les fonctions de « contrôleur en chef » ;
- D'assurer, le cas échéant, la communication dans l'exercice ;
- D'ordonner la fin de l'exercice (message « FINEX »).

Après :

- De présider les réunions d'analyse (à chaud et différée) ;
- D'entériner, après validation du chef d'établissement, le retour d'expérience (RETEX)
- Dans le cadre d'un exercice impliquant la préfecture, la direction d'exercice et la direction de l'animation (DIRANIM) incombent aux représentants de cette dernière.

B. L'animation de l'exercice (DIRANIM)

Il peut s'agir du DIREX. Le DIRANIM peut surtout être le pilote identifié par la direction de l'établissement pour mener la politique d'exercice.

Il anime l'exercice par l'injection d'événements (inputs) et joue les actions simulées (notamment les sollicitations et réponses d'organismes qui ne participent pas à l'exercice).

Avant l'exercice, il s'entoure d'un groupe de travail/comité de pilotage dédié à la préparation de l'exercice.

C. Les joueurs

Les joueurs désignent les participants à l'exercice. Il s'agit des salariés et agents de l'établissement concernés, mais aussi potentiellement ceux d'autres services, administrations ou établissements (forces de l'ordre, moyens de secours, établissements voisins).

À ces personnes s'ajoutent éventuellement les figurants (plastrons) qui jouent le rôle du public.

D. Les évaluateurs et les observateurs

Ces deux fonctions ne participent pas à l'exercice. Les observateurs et les évaluateurs peuvent être choisis au sein l'équipe d'animation.

Leurs missions diffèrent. Les observateurs prennent note des réactions du personnel et du déroulement général de l'exercice alors que les évaluateurs doivent s'appuyer sur des grilles d'évaluation.

Organiser un exercice de sûreté

I. Rétroplanning : les réunions à tenir avant l'exercice

Les principales réunions à tenir sont les suivantes :

- L'organisation à proprement parler de l'exercice débute par une réunion de planification (lancement de l'exercice).
- Des réunions intermédiaires sont organisées, ensuite, pour permettre aux différents groupes de travail de concevoir un projet de scénario. À leur issue, le comité de pilotage fait valider lors d'une réunion les propositions émanant des groupes de travail.
- Une réunion de finalisation vise à "boucler" la préparation de l'exercice avec les principaux acteurs.

II. Dossier d'exercice

A. Généralités

Le dossier d'exercice est le document récapitulatif et détaillé de l'organisation générale de l'exercice et de ses modalités d'exécution.

Il peut contenir les éléments suivants.

1. *Un tableau des personnes engagées*

   La liste exhaustive des organisateurs, joueurs, scénaristes et évaluateurs permettra de connaître avec précision le nombre et la nature des personnels engagés.

2. *Un scénario*

   Le dossier d'exercice comprendra une fiche descriptive de celui-ci, étant entendu qu'il ne s'agit nullement de décrire in extenso le scénario qui ne sera découvert par les joueurs que le jour de l'exercice.

   Le scénario peut se dérouler en temps réel ou bien en temps compressé. Dans ce dernier cas, il devra en être fait mention dans les conventions d'exercice.

3. *Des conventions d'exercice*

   Chaque convention d'exercice doit être rappelée explicitement afin de connaître les limites d'organisation de l'exercice (ce qui sera joué, simulé ou hors du champ de l'exercice). Les limites physiques de l'exercice doivent être anticipées en relation avec les autorités locales et préfectorales.

4. *Un dossier communication*

   En fonction du choix du comité de pilotage, les types de communication seront reportés dans cette rubrique. Les différentes autorités ou personnalités susceptibles d'être présentes seront également mentionnées.

B. Le dossier d'animation

Élaboré par le groupe de travail "scénario/animation" sous la responsabilité du DIRANIM, le dossier d'animation doit comprendre :

- La désignation du local où l'équipe d'animation évoluera, local qui sera équipé des moyens de transmission nécessaires (téléphones, postes de radio, etc.) ;
- Le déroulement détaillé et chronologique de l'exercice (sous la forme d'un chronogramme indiquant les différents inputs : événements, sollicitations presse, etc.) ;
- La liste des matériels et vecteurs de transmissions ;
- Les conventions d'exercice.

C. Le dossier joueur

En fonction des objectifs à atteindre, le DIREX autorisera la divulgation de tout ou partie des renseignements contenus dans le dossier d'exercice.

Ainsi, le joueur pourra être tenu informé :

- Du thème général de l'exercice ;
- De la date, le cas échéant (cf. supra);
- Du lieu où il se déroulera.

En aucun cas il ne sera informé du déroulement du scénario et encore moins des différents incidents prévus.

III. La communication

La fonction communication dans un exercice couvre deux champs distincts : l'information des publics avant l'exercice et la communication au sein de l'exercice.

A. La communication à propos de l'exercice

La préparation d'un exercice implique d'informer les participants (dans le cadre d'un exercice annoncé, non-inopiné), les autorités et potentiellement le grand public.

B. La communication dans le cadre de l'exercice

Dans le cadre d'un exercice la communication est à la main de la direction d'exercice (DIREX, cf. supra). Elle concerne la réponse à d'éventuelles sollicitations de la part des médias (simulés) ou d'autorités (mairie, préfecture, ministère).

IV. La logistique de l'exercice

L'organisation d'un exercice de sûreté demande d'anticiper certains aspects logistiques :

- Les modalités d'accueil des différentes catégories d'acteurs (figurants, évaluateurs, etc.) ;
- Les moyens de communication (radios, annuaires) ;
- Les moyens d'identification des catégories d'acteurs (chasubles de couleur pour les fonctions DIREX, DIRANIM, animation, évaluation, observation) ;
- L'identification de locaux spécifiques pour la gestion de la crise.

Évaluer des exercices

Dans la logique d'un cercle vertueux de préparation aux crises, il est essentiel d'évaluer l'exercice. L'outil le plus couramment utilisé est le retour d'expérience (RETEX).

On peut distinguer deux types de RETEX en fonction du moment où il se déroule : juste après l'exercice ou dans le cadre d'une réunion ultérieure.

I. RETEX à chaud

Il s'agit d'une réunion organisée immédiatement après l'exercice, se déroulant dans la convivialité et dans un lieu défini au cours de la préparation.

Cet échange permet de :

- Remercier les participants ;
- Dégager des remarques générales sur le déroulement de l'exercice ;
- Permettre aux joueurs, de décrire leur perception de l'exercice et leurs impressions personnelles sur son déroulement ;
- De prendre note des différentes remarques formulées pour compléter le rapport des évaluateurs et des observateurs.

Elle doit être courte sous peine de ne pas être écoutée. Le temps n'est pas à la recherche de solutions, mais à l'expression d'un ressenti sur l'exercice.

II. RETEX à froid

Chaque évaluateur transmet son analyse selon des critères qui ont été définis et écrits dans le dossier d'animation. Le pilote de l'exercice en fait la synthèse qu'il soumet au DIREX puis la présente en réunion plénière si besoin.

En fonction du niveau d'importance de l'exercice, il peut y avoir plusieurs réunions, si nécessaire, pour procéder au décorticage des différentes phases jouées pour retirer tous les enseignements possibles servant à entériner ou à modifier les procédures en vigueur mais aussi à améliorer l'organisation des exercices futurs.

Dès lors que plusieurs organisations coopèrent dans l'exercice, la procédure de RETEX peut avantageusement intégrer ces différents acteurs au cours d'une ou de plusieurs réunions synthétisant les observations des structures participantes.

III. Les leçons tirées des RETEX

L'enclenchement du cercle vertueux évoqué en introduction suppose d'identifier les axes d'améliorations au terme de ce processus de retour d'expérience.

En effet, les enseignements tirés des exercices doivent permettre d'améliorer les pratiques professionnelles (en adaptant les fiches réflexes par exemple) et de faciliter l'organisation de futurs exercices.

CHECKLIST

Planifier

Choix de l'exercice

☐ Sur table

☐ De terrain

☐ Annoncé

☐ Inopiné (suppose une maîtrise du sujet)

☐ En formation restreinte (jour de fermeture)

☐ En présence du public (difficulté supplémentaire)

Objectifs

Objectif principal				
Objectifs secondaires				
Objectifs spécifiques				

Acteurs

☐ Direction de l'exercice (DIREX) : . . . . . .

☐ Animation de l'exercice (DIRANIM) : . . . . . .

☐ Joueurs : . . . . . .

☐ Figurants (plastrons) : . . . . . .

☐ Évaluateurs et les observateurs : . . . . . .

CHECKLIST

Organiser

Rétroplanning

☐ Réunion de planification : . . . . . .

☐ Réunions intermédiaires : . . . . . .

☐ Réunion de finalisation : . . . . . .

Dossier d'exercice

☐ Personnes engagées : . . . . . .

. . . . . .

. . . . . .

☐ Scénario : . . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

☐ Conventions d'exercice : . . . . . .

. . . . . .

. . . . . .

☐ Dossier communication : . . . . . .

. . . . . .

. . . . . .

CHECKLIST

☐ Dossier d'animation : . . . . . .

. . . . . .

. . . . . .

☐ Désignation du local : . . . . . .

. . . . . .

. . . . . .

☐ Déroulement détaillé et chronologique de l'exercice . . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

☐ Matériels et vecteurs de transmissions (liste)

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

☐ Conventions d'exercice : . . . . . .

. . . . . .

CHECKLIST

☐ Dossier joueur

- Thème général de l'exercice :. . . . . .

. . . . . .

. . . . . .

- Date : . . . . . .
- Lieu : . . . . . .

Logistique

☐ Modalités d'accueil des acteurs :. . . . . .

. . . . . .

. . . . . .

☐ Moyens de communication (radios, annuaires). . . . . .

. . . . . .

. . . . . .

☐ Moyens d'identification des catégories d'acteurs (chasubles de couleur pour les fonctions DIREX, DIRANIM, animation, évaluation, observation).

. . . . . .

. . . . . .

☐ Locaux spécifiques pour la gestion de la crise. . . . . .

. . . . . .

. . . . . .

CHECKLIST

Évaluer des exercices

RETEX à chaud

☐ Remercier les participants

☐ Dégager des remarques générales sur le déroulement de l'exercice

☐ Perception de l'exercice et impressions des joueurs sur son déroulement

. . . . . .

. . . . . .

. . . . . .

. . . . . .

☐ Remarques formulées pour compléter le rapport des évaluateurs et des observateurs

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

RETEX à froid

☐ Analyse de l'évaluateur selon des critères qui ont été définis et écrits dans le dossier d'animation

☐ Réunions synthétisant les observations des structures participantes

Liens utiles

Exercices de sécurité civile | interieur.gouv.fr

FICHE PROCÉDURALE

OA4

CHAÎNE D'ALERTE FACE À UNE MENACE

ÉTAPE 1 : Diffusion initiale de l'alerte

Il s'agit dans un premier temps d'identifier la survenue d'une menace et de la signaler.

Qui ? : L'alerte de la survenue d'une menace doit être transmise par un personnel de l'établissement, donc formé. Il devra préciser autant que possible la nature de la menace, le volume à considérer ainsi que l'attitude du ou des personnes à considérer. Ces informations permettront de déterminer la situation de référence du PSE à retenir.

Pour éviter tout risque de fausses alertes, de paniques et de manière plus générale de conduites inappropriées, le public ne doit pas pouvoir être à l'origine de cette alerte, sauf à se rapprocher d'un personnel.

Avec quoi ? : Une solution technique fixe ou nomade et/ou humaine peut faciliter la diffusion de l'alerte.

ÉTAPE 2 : La gestion de l'alerte

Il s'agit d'identifier la situation de référence apparentée à la menace signalée.

Qui ? : L'alerte est transmise au directeur d'établissement ou à toute personne habilitée par ce dernier et spécialement formé sur ce sujet.

À partir de l'information recueillie et de toutes celles qu'il peut avoir par ailleurs (vidéoprotection, moyens techniques divers, comptes rendu d'autres agents, etc.) cette personne identifie la situation de référence la plus proche et déclenche le scénario de réponse associé permettant de faire prendre en compte le comportement adapté. En parallèle, elle prévient les forces de sécurité intérieure via l'appel **17**.

Avec quoi ? : Une solution technique fixe ou nomade et /ou humaine peut faciliter le traitement de l'information et l'identification de scénarios à déclencher.

Pour les établissements dotés d'un système technique de traitement de l'information, qu'il soit fixe ou nomade, un délai peut être envisagée en lien avec les forces de sécurité intérieure locale, pour permettre de préciser l'événement. Cette possibilité ne peut être envisagée que sous réserve du niveau de formation des agents de sécurité, de leurs équipements, voire de la nature de la menace identifiée. Ce délai ne devra pas excéder 5 min (délai à définir avec les forces de sécurité intérieure pour l'établissement) et devra être court-circuitée en cas de signalements multiples.

ÉTAPE 3 : Diffusion de l'alarme

Il s'agit de provoquer un comportement approprié chez les personnes situées dans l'établissement.

Qui ? : L'alarme doit pouvoir être transmise par un moyen technique et/ou humain capable de provoquer l'évacuation et/ou le confinement des personnes présentes en fonction de leurs positions, avec comme objectifs de limiter la panique et le nombre de victimes sur la base de scénarios préétablis et de l'analyse de la situation en cours.

Avec quoi ? : Une solution technique fixe ou nomade et /ou humaine peut permettre une diffusion de l'alarme efficace, voire un rappel aux personnes sur les conduites à tenir.

CHECKLIST

Diffusion initiale de l'alerte par le personnel

☐ Nature de la menace : . . . . . .

. . . . . .

. . . . . .

. . . . . .

☐ Volume à considérer : . . . . . .

. . . . . .

. . . . . .

. . . . . .

☐ Attitude du ou des personnes à considérer : . . . . . .

. . . . . .

. . . . . .

. . . . . .

Gestion de l'alerte

☐ Transmettre l'alerte au directeur d'établissement ou toute personne habilitée par lui

☐ Identifier la situation de référence la plus proche et déclencher le scénario de réponse associé

☐ Prévenir les forces de sécurité intérieure : Voir FICHE RÉACTION : R1 « ***Prévenir les autorités*** »

Diffusion de l'alarme

☐ Déclencher l'alarme

☐ Ordonner l'évacuation ou le confinement

☐ Limiter la panique

FICHE PROCÉDURALE

OA5

VÉRIFICATION DU PERSONNEL

Les recommandations figurant dans cette fiche sont à adapter en fonction du lieu, de la nature, de l'importance et de la durée de l'événement auquel elles peuvent s'appliquer.

Certaines menaces extérieures, qu'elles émanent de criminels, de terroristes ou de concurrents cherchant à acquérir un avantage commercial, sont susceptibles de s'appuyer sur la collaboration de « quelqu'un de l'intérieur ».

Il peut s'agir d'un salarié, ou de tout employé contractuel ou intérimaire (agent d'entretien, traiteur, agent de sécurité, etc.) autorisé à accéder à vos locaux. Dans le cas d'un salarié, il peut s'agir d'une personne qui travaille déjà pour vous, ou d'une nouvelle recrue ayant infiltré votre organisation dans le but d'obtenir des informations ou de tirer parti de l'autorisation d'accès que l'emploi peut offrir.

En quoi consiste la fiabilité du personnel ?

La fiabilité du personnel est un système de politiques et de procédures visant à gérer le risque d'une exploitation, par le personnel ou les contractants, de leur autorisation d'accès aux actifs ou aux locaux d'une organisation, à des fins non autorisées. Ces fins peuvent englober de nombreuses formes d'activité illégale, allant du menu larcin au terrorisme.

L'objectif de la fiabilité du personnel est de limiter les risques au maximum. Elle s'assure pour cela que les organisations emploient des individus dignes de confiance, en s'assurant de leur compétence professionnelle par la production de leurs diplômes professionnels ou techniques, en repérant les comportements suspects, et en résolvant les problèmes de sécurité lorsqu'ils se manifestent.

Comprendre et évaluer les risques relatifs à la fiabilité du personnel

Les organisations sont régulièrement confrontées à toutes sortes de risques. L'un d'eux concerne l'éventualité que des employés ou des contractants profitent de leur fonction au sein de l'organisation à des fins illégitimes. Ces risques peuvent être réduits, mais ne pourront jamais être entièrement évités. Comme pour de nombreux autres risques, l'organisation doit plutôt adopter un processus continu en vue de s'assurer qu'ils sont gérés de manière adéquate et rentable.

Contrôle préalable à l'emploi

La fiabilité du personnel repose sur un certain nombre de méthode de contrôle, utilisées dans le cadre du processus de recrutement, mais également de façon régulière pour le personnel existant. Les modes d'exécution de ce contrôle varient considérablement d'une organisation à l'autre ; certaines méthodes sont très simples, d'autres plus sophistiquées. Le contrôle préalable à l'emploi vise à vérifier les références des postulants et à s'assurer que ces derniers remplissent les conditions légales pour remplir l'emploi considéré. Lors de la réalisation de ces vérifications, il sera déterminé si le postulant a dissimulé des informations importantes ou s'est présenté sous un faux jour.

Pour les personnels mis à disposition par une société privée de sécurité, il s'agit de se rapprocher du CNAPS (Conseil National des Activités Privées de Sécurité) ou de ses délégations régionales pour vérifier si la société prestataire de service et/ou son ou ses employés mis à disposition remplissent bien les conditions légales pour remplir la mission confiée. Le cahier des charges fixant les conditions contractuelles pourra inclure des clauses veillant au respect des règles de fiabilité.

Identité

De toutes les vérifications préalables à l'emploi, celle de l'identité est la plus fondamentale entraînant une vérification portant sur les principales pièces d'identité et/ou cartes de séjour.

Diplômes

La vérification des diplômes professionnels peut aider à identifier les postulants qui essaient de dissimuler des informations défavorables.

Lors de la confirmation des informations relatives aux diplômes d'un individu, il est toujours important de :

- Se demander si le poste exige une vérification des diplômes ;
- Systématiquement réclamer les diplômes originaux et en faire une copie ;
- Comparer les informations mentionnées sur les diplômes et autres documents avec celles fournies par le postulant ;
- Confirmer indépendamment l'existence de l'établissement du diplôme et le contacter pour vérifier les renseignements fournis par le postulant.

Recrutement des intérimaires

Les organisations emploient un large éventail d'agents intérimaires (personnel informatique, agents d'entretien, conseillers en gestion, etc.). Il est important de s'assurer que les contractants sont soumis au même degré de contrôle préalable à l'emploi que les salariés permanents bénéficiant de niveaux d'accès équivalents aux actifs de l'entreprise, qu'il s'agisse des locaux, des systèmes, des informations ou du personnel.

Fiabilité des intérimaires

Lors de la gestion des risques liés à la présence d'intérimaire sur place, il est important de :

- S'assurer que les vérifications préalables à l'emploi sont de même niveau que celles réalisées pour les employés permanents ; si cela se révèle impossible, en raison d'échéances serrées ou d'un manque d'informations disponibles pour la vérification des antécédents, les risques qui en découlent doivent alors être gérés de façon efficace ; de préférence, la mise en œuvre de toute mesure de sécurité supplémentaire s'appuiera sur une évaluation des risques de sécurité du personnel ;
- Lorsque les vérifications préalables à l'emploi, ou toute autre mesure se rapportant à la fiabilité du personnel, sont effectuées par un organisme contractant et non par l'organisation employeuse, une description détaillée des vérifications à entreprendre et des normes fixées doit être incluse dans le contrat établi entre les deux ; le processus de vérifications préalables à l'emploi appliqué par le contractant doit en outre faire l'objet d'audits réguliers ; vérifiez que la personne envoyée par l'organisme contractant est bien la personne qui se présente au travail (en contrôlant ses papiers ou en ayant recours à un service électronique de contrôle de l'identité par exemple).

Une fois que l'intérimaire aura commencé à travailler au sein de l'organisation, il devra être géré de manière sûre. Les étapes suivante vous y aideront :

- Procédez à une évaluation des risques en vue de déterminer les menaces et le niveau de risque associés à la commission par l'intérimaire d'actes malveillants dans le cadre de ses fonctions ;
- Assurez-vous que le contrat établi entre l'organisation et l'intérimaire, soit entre l'organisation et l'organisme contractant, définit les codes de pratiques et les normes qui s'appliquent ;
- Fournissez des badges avec photo aux agents contractuels et aux employés intérimaires, et stipulez qu'ils doivent être portés en permanence ; dans l'idéal, l'organisation employeuse devrait conserver les badges des contractants entre chacun de leurs visites, et ne les délivrer de nouveau à chaque fois qu'après avoir vérifié l'identité du contractant : l'organisation employeuse et l'organisme contractant (ou le contractant, si aucun organisme n'est impliqué) doivent convenir d'une procédure visant à fournir du personnel temporaire en cas d'indisponibilité du contractant : ces dispositions doivent être incluses dans le contrat établi entre les deux parties et l'organisation employeuse devra décider des mesures additionnelles de sécurité du personnel à mettre en œuvre (accès restreint ou surveillé par exemple) lorsque le personnel remplaçant est sur le site ;

OA5 VÉRIFICATION DU PERSONNEL

- Si un intérimaire est en fonction, mais que les vérifications préalables à l'emploi requises n'ont pas été effectuées, ou si les résultats de ces vérifications ne sont pas entièrement satisfaisants, mais que l'expertise du contractant est à ce point nécessaire qu'il est employé de toute manière, il est alors indispensable de prévoir des mesures supplémentaires de sécurité du personnel (supervision permanente par exemple).

Le recours à la biométrie permet de limiter les risques de substitution.

OA5

VÉRIFICATION DU PERSONNEL

CHECKLIST

Contrôle préalable à l'emploi

Références des postulants : . . . . . .

. . . . . .

. . . . . .

Questions	Réponse			Remarques
	O	N	SO	(Description)
Les conditions légales sont-elles remplies pour l'emploi considéré ?				
Le postulant a-t-il dissimulé des informations importantes ?				
Le postulant s'est-il présenté sous un faux jour ?				

Fiabilité des intérimaires

☐ Les vérifications préalables à l'emploi sont de même niveau que celles réalisées pour les employés permanents

En cas de recrutement par un organisme contractant :

☐ La personne envoyée par l'organisme contractant est bien la personne qui se présente au travail

☐ Contrôler ses papiers d'identité

☐ Procédez à une évaluation des risques

☐ Le contrat établi entre l'organisation et l'intérimaire définit les codes de pratiques et les normes qui s'appliquent

☐ Fournissez des badges avec photo aux agents contractuels et aux employés intérimaires

☐ Stipulez que les badges doivent être portés en permanence

☐ Conserver les badges des contractants entre chacun de leurs visites

☐ Délivrer les badges qu'après avoir vérifié l'identité du contractant

Liens utiles

Gérer la sûreté et la sécurité des évènements et sites culturels | culture.gouv.fr

Charte de bonnes pratiques en matières d'achats de prestations de sécurité privée | interieur.gouv.fr

FICHE PROCÉDURALE

OA6

PRÉPARER SA COMMUNICATION DE CRISE

Trois temps fondamentaux de la communication :

L'explication – Quoi ? Comment ?

Comment cela a-t-il pu se passer ?

Les médias essayent de comprendre comment cela a pu arriver. C'est la chasse aux sources. Les communicants doivent obtenir des informations fiabilisées pour donner la version des faits de l'organisation.

La compassion envers les « victimes » perçues

Attention aux schémas de « victimisation » en France dans lesquels on reconnait plus facilement l'individu comme victime que l'entreprise ou l'État.

Les médias se focalisent sur les victimes et l'impact de la crise sur leur vie. C'est la chasse aux témoignages. Les communicants doivent donc intégrer des messages d'empathie dans leur stratégie de communication.

La responsabilité et la réparation – La faute à qui ?

Qui va payer ? Dédommager ?

Les médias cherchent à identifier celui qui devra dédommager. C'est la chasse au responsable. L'organisation doit assumer ses responsabilités si elle est mise en cause.

Si ces trois temps se retrouvent régulièrement dans les stratégies de communication de crise mises en place, aucune crise n'est la même. Le principe à privilégier est donc celui de l'adaptation, de la réflexion et du bon sens.

Attention à prendre la parole dans le bon tempo !

- Parler de « réparation » en phase de « compassion », c'est risquer d'apparaître comme « froid », « insensible », « peu préoccupé par le malheur des gens ».
- Parler de « compassion » lors de la phase de « réparation », c'est risquer d'apparaître comme « manipulateur », voulant « fuir ses responsabilités ».

Les comportements clés

Prévision

Différence entre soudaineté (je sais que ça peut arriver mais je ne sais pas quand) et imprévisibilité (je n'imaginais pas que cela puisse arriver). Un organisme se doit aujourd'hui d'avoir préparé les crises les plus « probables ».

Respect et compassion

Il faut toujours avoir du respect et de la compassion pour la victime, quel que soit le contexte de la crise.

Une règle d'or : communiquer

Si l'institution représentée ne parle pas, quelqu'un le fera à sa place. Il est essentiel de prendre la parole pour préempter une partie du discours.

Il est difficile de concevoir une information sans l'image qui va avec (il faut voir pour croire). La communication de crise doit donc donner à voir.

2015 a également marqué un tournant en termes de gestion et de communication en cas de crises majeures. Les crises se succèdent à une fréquence bien plus élevée et leur gravité est également beaucoup plus importante. Cela a fait évoluer, et continue aujourd'hui de faire évoluer, les procédures et stratégies de réponse tant en termes de gestion que de communication de crise.

Les attentes du public

Le public souhaite :

Être informé

Il faut donner à ses publics l'information nécessaire dont ils ont besoin en fonction de leurs domaines d'intérêts et de leurs préoccupations.

Un discours responsable

Il s'agit de tenir un discours clair, concret qui :

- Permet à l'interlocuteur d'obtenir la perception la plus complète possible des risques éventuels ;
- Offre une présentation objective des conséquences possibles de la situation ;
- Précise les éléments connus et inconnus (on a tout à fait le droit de dire que l'on ne sait pas, mais dans ce cas, il faut préciser quand est-ce que les informations manquantes seront disponibles) ;
- Explique les actions mises en place pour résoudre au plus vite la situation.

Éviter les écueils

Vouloir minimiser la situation :

- La volonté d'éviter « la panique » ou « d'en dire le moins possible » au contraire génère le plus souvent de l'inquiétude et du stress chez vos interlocuteurs ;

Omettre volontairement des éléments essentiels :

- Le mensonge par omission est bien considéré au même plan que le mensonge, etc. et a pour conséquence la décrédibilisation immédiate de l'émetteur (si l'on ment c'est bien que l'on a quelque chose à cacher, et si l'on a quelque chose à cacher c'est donc que l'on est coupable).

Être rassuré

- Donner des informations précises sur l'état de la situation, lister le « connu » et « l'inconnu ».
- Faire des points réguliers et surtout indiquer quand le prochain point d'information aura lieu.

Il ne s'agit pas de rassurer absolument ses publics sur la situation mais plutôt sur la capacité à gérer la situation.

Être considéré

Toujours prendre en considération son interlocuteur, même si ses inquiétudes ou ses requêtes ne vous semblent pas fondées ou pertinentes. Le ton de la communication est essentiel.

Gérer les publics en situation de crise

Établir un plan d'action

Prendre en compte tous les publics identifiés :

- Se fonder sur le travail d'identification des publics réalisé en amont ;
- Ajouter immédiatement les nouveaux publics au fur et à mesure de leur apparition dans le déroulement de la crise :
  - Anciens salariés ;
  - « Experts » réels ou auto-proclamés ;
  - « Représentants » de victimes ;
  - Associations de riverains ;
  - Etc.

Distinguer le court et moyen terme :

- Identifier les publics prioritaires :
  - Les plus utiles pour la résolution de la crise (il ne s'agit pas forcément des plus favorables, etc.) ;
  - Les plus influents / les plus médiatiques.

Attention en situation de crise, la tentation est de faire d'abord ce qui est « facile » plutôt que ce qui est « utile ». Par exemple, il est plus facile de s'adresser en priorité aux personnes que l'on connait bien, mais est-ce bien la démarche la plus utile ?

- Définir pour chacun d'eux un ordre de priorité en se fondant sur la matrice d'Eisenhower

01 **Important & urgent** Public prioritaire	**02** **Important & non-urgent** à traiter absolument
03 **Pas important & urgent** Attention à ne pas trop se focaliser au risque de perdre du temps	**04** **Pas important & non-urgent** Ne pas consacrer de moyens dans l'immédiat

Définir pour chacun des publics la stratégie à mettre en place

- Les alerter de la crise ;
- Les associer à la gestion de crise ;
- Les informer ;
- Les isoler (pour des publics opposés par exemple).

Définir la stratégie en fonction de l'objectif à atteindre

- S'assurer de leur coopération, de leur mobilisation parce qu'ils peuvent aider à la résolution de la crise ;
- Susciter leur silence, leur neutralité, voire leur inaction ;
- S'assurer que des opposants ne viennent pas rendre la gestion de la crise plus complexe par des interventions inappropriées ;
- Dans certains cas il peut être utile de s'assurer du « silence » des médias ou de certains élus : cela est tout à fait possible tant que cette requête est « justifiée » et parait indispensable à la bonne gestion de la crise.

Les éléments d'un bon discours

S'adresser efficacement à ses publics c'est :

- **L'empathie :** Un mot pour les victimes ;
- **La prise de responsabilité :** Ne pas se dérober, avoir une attitude responsable. Ne pas confondre la responsabilité morale (déterminée par l'opinion publique immédiatement) et la responsabilité juridique (déterminée par le juge lors d'un éventuel procès) ;
- **La clarté et la collaboration :** Annoncer la collaboration avec les parties prenantes ;
- **La résolution (le futur) :** Expliquer ce qui est mis en place pour s'assurer que ça ne se reproduise pas.

FICHE PROCÉDURALE

OA7 CONSEILS AUX VOYAGEURS

Avant le départ

S'informer

Sur la sécurité dans le pays :

- La rubrique « Conseils aux voyageurs » du site Internet du ministère de l'Europe et des affaires étrangères vous informe sur les risques propres à chaque pays et les précautions à prendre.
- Les fiches pays vous renseignent sur les problèmes de sécurité, la fiabilité des moyens de transport, les risques sanitaires et les conditions d'hygiène locale, les us et coutumes et la législation locale.
- Il est important de choisir un circuit touristique ou un lieu de villégiature qui offre le maximum de sécurité. Les cartes de la rubrique « Conseils aux voyageurs » vous indiquent, pour chaque pays, le degré de sécurité de ses différentes régions.
- Les zones rouges sont formellement déconseillées, car elles peuvent représenter un risque élevé pour votre vie et votre sécurité.
- Les zones oranges sont déconseillées sauf raisons impératives (professionnelle ou familiale).

Planifier

- Il est nécessaire de souscrire aux assurances adaptées (notamment rapatriement / hospitalisation) lorsque vous vous rendez à l'étranger.
- Pensez à enregistrer les numéros d'urgence locaux, de votre assurance et du consulat. Il existe des services consulaires dans la plupart des pays.

Inscrivez-vous sur le service en ligne gratuit « ARIANE »

Pourquoi s'inscrire ?

Créé par le ministère de l'Europe et des affaires étrangères, le site Ariane permet à tout ressortissant français, lors d'un voyage ou d'une mission ponctuelle à l'étranger, de se signaler afin de bénéficier, par mail, SMS ou téléphone, d'informations et de consignes de sécurité en temps réel dans le pays de villégiature. Ariane permet également aux autorités françaises, en cas de crise, de connaître votre présence dans un pays.

http://diplomatie.gouv.fr/ariane

L'inscription sur le site Ariane, conçue en concertation avec la CNIL, offre toutes les garanties de sécurité et de confidentialité des données personnelles. Elle ne se substitue pas à l'inscription au registre des Français établis hors de France dès lors que le temps de séjour est supérieur à 6 mois.

Pour plus d'informations vous pouvez vous rendre sur le site du ministère de l'Europe et des affaires étrangères :
https://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/

En cas d'attaque terroriste

Si jamais vous êtes confronté à une attaque terroriste à l'étranger, vous devez, comme vous le feriez en France, adapter vos réactions 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.

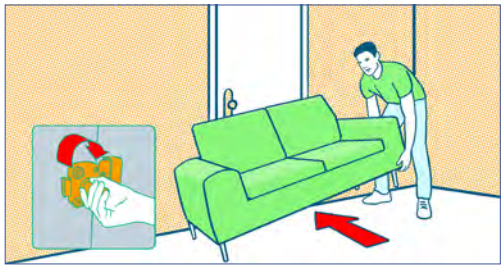
S'échapper

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.

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 (numéro d'appel d'urgence européen : **112** ; ou **numéro spécifique du pays** où vous vous trouvez) ;
- **Où ?** Donnez votre position mais également celle de vos agresseurs ;
- **Quoi ?** Nature de l'attaque, estimation du nombre d'assaillants, description (sexe, vêtements, physionomie, signes distinctifs, etc.), attitude (comment se comportent-ils, regardent-ils la télévision, ont-ils des moyens de communication, etc.).
- **Suivez les consignes des autorités locales :** elles sont responsables de la sécurité des personnes se trouvant sur leur territoire, quelle que soit leur nationalité.

Après une attaque

- **Informez vos proches de votre situation, quand cela est possible, par tous les moyens à disposition (SMS, appels, réseaux sociaux) ;**
- **Contactez le 116 006, plateforme téléphonique nationale d'écoute et d'information des victimes ;**
- **Hors France métropolitaine, composez-le +33 (0)1 80 52 33 76 (numéro non surtaxé) ;**
- Des écoutants professionnels vous offrent une écoute privilégiée, une identification des besoins et des premiers conseils, 7 jours sur 7 ;
- Vous pourrez être mis en relation avec une association d'aide aux victimes et/ou tout service ou administration susceptible de répondre à vos demandes.

116 006
Service & appel gratuits 7/7j
Numéro d'aide aux victimes

Liens utiles

Conseils aux voyageurs | diplomatie.gouv.fr

Comment préparer ses déplacements et voyages à l'étranger ? | sgdsn.gouv.fr

RÉACTION

R1 | Prévenir les autorités 79
R2 | Attaques armées. 81
R3 | Prise d'otages. 85
R4 | Produits toxiques 86
R5 | Drones malveillants 90
R6 | Cyberattaque 92
R7 | Signalement d'un individu suspect 94
R8 | Fouille des locaux 99

FICHE PROCÉDURALE

R1 RÉACTION | PRÉVENIR LES AUTORITÉS

Pour le contact des forces de sécurité intérieure

En présence d'un événement grave, l'alerte des services de police ou de gendarmerie est réalisée dans les plus brefs délais.

L'alerte est faite par le directeur d'établissement ou un agent formé et désigné par ses soins. Pour cela, l'agent dispose d'un téléphone dédié au _____

A défaut, tout autre moyen de communication rapide et sûr peut être utilisé.

L'agent :

1. Décroche le téléphone et compose le **n°17** ou envoie un **SMS** au **114** ;
2. Dès la liaison établie, suit la **trame du message d'alerte :**

A. Identification

[Mon nom, ma fonction], je suis à **[nom de l'ES]**, mon n° de téléphone pour être rappelé est le : **[numéro de téléphone].**

B. Type d'événement et risques

Nous sommes en présence de :

☐ agression physique ☐ fusillade ☐ explosion

☐ colis suspect ☐ autre (préciser) . . . . . .

C. Adresse exacte

Nous sommes au **[adresse du site].** L'accès des secours se fera par : **[adresse et description du point d'accès].**

D. Nombre de public (patients et visiteurs) et de personnels sur site

Nous sommes **[XX personnes, dont XX non autonomes].**
Il n'y a pas (ou il y a **[XX]**) de blessé ou mort.

E. Actions effectuées

☐ évacuation ☐ confinement de patient

☐ premiers secours ☐ autre (préciser) . . . . . .

NE PAS RACCROCHER EN PREMIER

Connaître les numéros d'urgence

Les numéros d'**appel d'urgence** permettent de **joindre gratuitement les secours 24h/24**

Service	Numéro à composer	Dans quel cas ?
Numéro d'appel d'urgence européen	**112**	Si vous êtes victime ou témoin d'un accident dans un pays de l'Union Européenne
Le Service d'aide médicale urgente (SAMU)	**15**	Pour obtenir l'intervention d'une équipe médicale lors d'une situation de détresse vitale, ainsi que pour être redirigé vers un organisme de permanence de soins
Police-Secours	**17**	Pour signaler une infraction qui nécessite l'intervention immédiate de la police ou de la gendarmerie
Sapeurs-pompiers	**18**	Pour signaler une situation de péril ou un accident concernant des biens ou des personnes et obtenir leur intervention rapide
Numéro d'urgence pour les personnes sourdes et malentendantes	**114**	Si vous êtes victime ou témoin d'une situation d'urgence qui nécessite l'intervention des services de secours. Numéro accessible par FAX et SMS

Liens utiles

Fiche message d'alerte - Guide d'aide à l'élaboration d'un PSE - p. 37 | solidarites-sante.gouv.fr

Signalement de situations suspectes – Recommandation à l'usage du public | sgdsn.gouv.fr

Prévention et signalement des cas de radicalisation djihadiste | sgdsn.gouv.fr

FICHE PROCÉDURALE

R2

RÉACTION | ATTAQUES ARMÉES

Réagir en cas d'attaque terroriste – Alerter | sgdsn.gouv.fr

Une attaque armée est exécutée par un ou plusieurs individus dont l'intention est soit de faire un maximum de victimes sans distinction, soit de cibler spécifiquement certaines personnes ou lieux symboliques. Les agresseurs peuvent utiliser principalement des armes à feu, des armes blanches (couteau, hache) ou des ceintures explosives.

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

Généralités :

- Déterminer la réponse la plus appropriés à la situation. Celle-ci n'est pas figée, elle évolue : adoptez vos modes de réaction aux circonstances.
- ***Si l'attaque est extérieure au site dans lequel vous vous trouvez,*** il est recommandé de rester à l'abri.
- ***Si l'attaque a lieu à l'intérieur du site où vous vous trouvez,*** respectez les consignes de sécurité présentées ci-dessous.

1. S'échapper

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

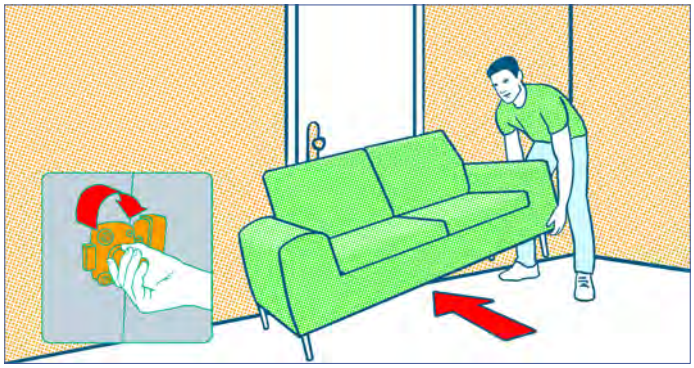
Condition 2 : *Être certain de pouvoir vous échapper sans risque.*

Si ces conditions sont remplies :

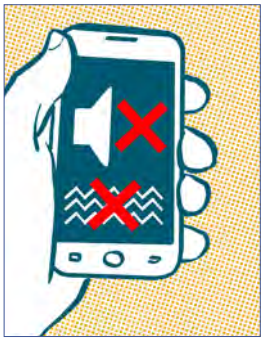
- Ne déclenchez pas l'alarme incendie
- Laissez toutes vos affaires sur place
- Ne vous exposez pas (courbez-vous)
- Prenez la sortie la moins exposée
- Utilisez un itinéraire connu
- Aidez les autres personnes à s'échapper
- Prévenez / Alerter les personnes
- Évitez les mouvements de panique
- Facilitez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

2. Se cacher

Dans la mesure où vous ne pouvez pas vous échapper :



- Enfermez-vous et barricadez vous : Condamner la porte si celle-ci n'a pas de serrure en bloquant la poignée avec des moyens de fortune (meuble, etc.)
- Éloignez-vous de la fenêtre
- Mettez les portables sur silencieux et décrochez les téléphones fixes
- Éteignez les lumières
- 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)



- Restez proches et rassurez les personnes manifestant un stress
- Restez le plus silencieux et discret possible jusqu'à l'intervention des forces de sécurité

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, etc.)
- **Qui ? :** Nombre d'assaillants, description physique et attitude, estimation du nombre de personnes blessées ou cachées.
  - Comment se comportent-ils ?
  - Regardent-ils la télévision ?
  - Quels moyens de communications ont-ils ?
  - **NE RACCROCHEZ PAS !**
  - 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 !

4. Résister

Si se cacher ou évacuer est impossible, et si votre vie est 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.

- Tentez de neutraliser le terroriste à plusieurs
- Distrayez l'adversaire (criez)
- Profitez d'un moment de vulnérabilité de l'agresseur pour l'attaquer (changement de chargeur, etc.)
- Protégez-vous avec un bouclier de fortune (sac, vêtement enroulé autour de l'avant bras).

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

5. Facilitez l'intervention des forces de sécurité et des services de secours

Afin de facilitez 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 blessez 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.

Liens utiles

Plaquette VIGIPIRATE | sgdsn.gouv.fr

Réagir en cas d'attaque terroriste | gouvernement.fr

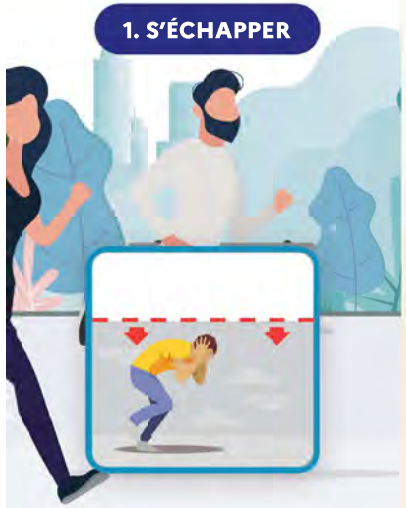
Les gestes d'urgence | gouvernement.fr

Réagir en cas d'attaque

PREMIER MINISTRE
Liberté
Égalité
Fraternité

Réagir en cas d'attaque

1. S'ÉCHAPPER



ÊTES-VOUS CERTAIN DE POUVOIR VOUS ÉCHAPPER SANS RISQUE ?

SI OUI

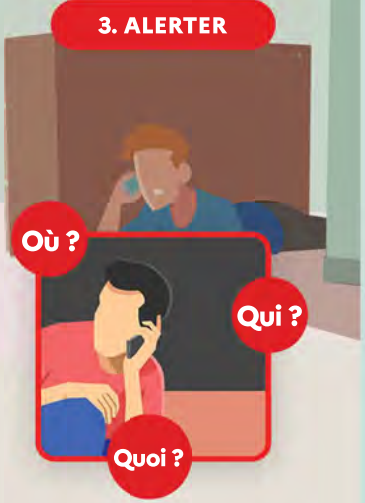
- Ne déclenchez pas l'alarme incendie
- Laissez toutes vos affaires sur place
- Ne vous exposez pas (courbez-vous)
- Prenez la sortie la moins exposée
- Utilisez un itinéraire connu
- Aidez les autres personnes à s'échapper
- Prévenez / alertez les personnes
- Évitez les mouvements de panique
- Facilitez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

FAIRE FACE ENSEMBLE

FICHE PROCÉDURALE

R3

RÉACTION | PRISE D'OTAGES

Les prises d'otage sont un des modes opératoires utilisés principalement par les mouvements terroristes, mais aussi potentiellement par la petite délinquance ou le crime organisé quand les malfaiteurs perdent le contrôle de la situation. Elles sont majoritairement résolues en quelques heures sur le territoire national. Cependant, il convient de suivre quelques consignes simples afin d'assurer votre sécurité et celle des autres personnes retenues.

Si vous êtes retenus de force par un ou plusieurs individus armés, essayez dans la mesure du possible de :

- Gardez votre calme et rassurez les plus fragiles sauf si on vous interdit de communiquer entre otages.
- N'utilisez pas vos téléphones portables.
- Facilitez l'intervention des forces de sécurité et des services de secours : obéissez aux consignes et en cas d'assaut des forces de l'ordre, allongez-vous par terre et ne faites pas de gestes brusques. Laissez vos mains apparentes.
- Repérez discrètement les sorties et les abris possibles en cas de fusillade.
- Suivez les instructions des terroristes : ne soutenez pas leur regard et ne les provoquez pas, sans pour autant être suppliant ou servile.
- Dans la mesure du possible, mémorisez toutes les informations susceptibles d'aider les enquêteurs : apparence physique, noms, tenue vestimentaire, armes, conversations, etc.

Liens utiles

Plaquette VIGIPIRATE | sgdsn.gouv.fr

FICHE PROCÉDURALE

R4

RÉACTION | PRODUITS TOXIQUES

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

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

- **Protégez votre nez et votre bouche par tous les moyens possibles** : mouchoir, foulard ou tissu humides.
- Même si vous vous sentez mal, **ne vous allongez pas, ne vous asseyez pas**, vous pourriez ne plus vous relever.
- **Quittez rapidement les lieux** semblant présenter un danger (si odeur anormale, si des personnes larmoient ou font des malaises, etc.).
- 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.
- **Une fois à distance et à l'abri, retirez délicatement votre première couche de vêtements**, sans en toucher l'extérieur et cherchez à les isoler, si possible dans un sac plastique (type sac poubelle) ou sinon les mettre au sol à distance de soi et les indiquer à l'arrivée des secours. Si vous le pouvez déshabillez-vous complètement et lavez-vous les mains à l'eau et au savon.
- **Utilisez votre portable uniquement pour alerter les secours** en précisant votre emplacement et s'il faut intervenir rapidement sur un cas grave.
- **Ne rentrez surtout pas chez vous. Ne vous rendez pas de vous-même à l'hôpital**. Attendez impérativement les secours et suivez leurs consignes, vous risqueriez de contaminer vos proches !
- Les services de secours organisent un **point de rassemblement** 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 et des soins

Attention : Certains symptômes graves peuvent survenir plusieurs heures après l'intoxication. Dans ce cas, appelez sans tarder le 15, rappelez que vous étiez dans la zone toxique et suivez les consignes que l'on vous donnera.

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

Liens utiles

Produits chimiques – Signalement de tout vol ou utilisation suspecte | sgdsn.gouv.fr

Que faire en cas d'exposition à un gaz toxique | sgdsn.gouv.fr

QUE FAIRE EN CAS D'EXPOSITION À UN GAZ TOXIQUE

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

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

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

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

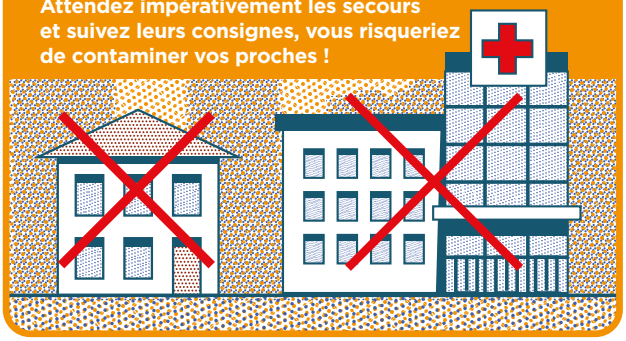
4 Si vous apercevez des gens en train de s'évanouir ou de suffoquer, aidez-les à sortir de la zone sans revenir sur vos pas.

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

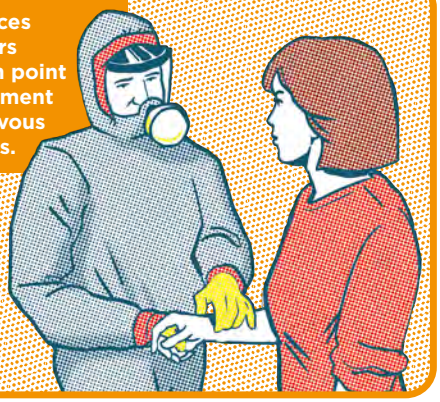
6 Utilisez votre portable uniquement pour alerter les secours en précisant votre emplacement et s'il faut intervenir rapidement sur un cas grave.

Pompiers : 18 ou 112
SAMU : 15

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



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



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

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

ATTENTION !

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

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

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

VIGIPIRATE

FICHE PROCÉDURALE

R5

RÉACTION | DRONES MALVEILLANTS

Un drone aérien, c'est un aéronef de type : aérostat, aéromodèle, montgolfière, planeur, dirigeable, hélicoptère, multirotor, autogire, convertible, voilure fixe, SANS PERSONNE A BORD.

Quelles sont les règles à connaître avant de faire voler un drone dans l'espace public ?

Je ne dois pas :

- **survoler** les personnes sauf pour des drones très légers (< 250g) ;
- **voler au-dessus de l'espace public** en agglomération sans notification préalable à la préfecture ;
- **perdre de vue** mon aéronef en vol ;
- **dépasser la hauteur** maximale de vol de 120 mètres ;
- **voler à proximité** des aéroports et aérodromes ;
- **survoler les sites** sensibles ou protégés ;

Je dois :

- **respecter** les conditions et restrictions applicables à la catégorie d'exploitation du drone (catégorie Ouverte ou Spécifique)
- **m'enregistrer** en tant qu'exploitant d'UAS : https://www.ecologie.gouv.fr/sites/default/files/enregistrement_exploitant_uas.pdf
- enregistrer le drone si celui-ci a une masse supérieure à 800 grammes : https ://alphatango.aviation-civile.gouv.fr
- me conformer à l'obligation de signalement électronique si le drone a une masse supérieure à 800 grammes : https ://www.ecologie.gouv.fr/sites/default/files/notice_signalement_electronique.pdf
- respecter les zones interdites de survol en consultant le site géoportail de la DGAC : https://www.geoportail.gouv.fr/donnees/restrictions-uas-categorie-ouverte-et-aeromodelisme
- respecter la vie privée d'autrui ;
- souscrire un contrat d'assurance prenant en compte mon activité ;
- consulter le site de la DGAC pour prendre connaissance de la réglementation en vigueur : www.ecologique-solidaire.gouv.fr/drones-loisir-et-competition
- respecter la réglementation en matière d'interdiction de prise de vue aérienne (arrêté du 27 octobre 2017).

Comment intégrer une activité drone durant mon évènement ?

- Je privilégie le recours à un professionnel déclaré : https://alphatango.aviation-civile.gouv.fr/login.jsp (en bas de la page web : « liste des exploitants déclarés »)

Je dois :

- proposer un cahier des charges en toute connaissance de la réglementation en vigueur ;
- stipuler l'activité drones dans le dossier de sécurité lors de ma déclaration à la préfecture ;
- définir un périmètre de sécurité pour les évolutions des drones afin de protéger les personnes au sol.

Comment se prémunir d'un usage malveillant de drone ?

Lors de la préparation de la réunion, je dois :

- inclure la menace-drone dans mon plan de sécurité et de secours ;
- me rapprocher des services de la préfecture afin d'identifier les éventuelles mesures de prévention à mettre en œuvre ;
- sensibiliser les agents de sûreté de la potentialité de la menace et des actions immédiates à déclencher (détection, alerte, réaction, compte-rendu).

Pendant la manifestation, je dois :

- coordonner l'activité des drones autorisés à voler ;
- informer le public des survols prévus de drones par tous moyens (affichage, message sonore, etc.) ;
- en cas de survol de drone non prévu :
  - rendre compte aux forces de sécurité intérieure (police ou gendarmerie) ;
  - si le drone est à terre, ne pas s'en approcher et établir un périmètre de sécurité.

Liens utiles

Drones : Règles d'utilisation et mesures de prévention face à un usage malveillant | sgdsn.gouv.fr

Guide incidents de drones – Notification et suivi | ecologie.gouv.fr

Vol de drones en agglomération – Réglementation | ecologie.gouv.fr

Où piloter son drone de loisir et quelles précautions en matière de vie privée | cnil.fr

FICHE PROCÉDURALE

R6

RÉACTION | CYBERATTAQUE

Vous n'avez pas eu le temps de mettre en œuvre les règles décrites dans ce guide ou les attaquants ont réussi à les contourner. Ne cédez pas à la panique, et ayez les bons réflexes.

- En cas de comportement inhabituel de votre ordinateur, vous pouvez soupçonner une intrusion (impossibilité de se connecter, activité importante, connexions ou activités inhabituelles, services ouverts non autorisés, fichiers crées, modifiés ou supprimés sans autorisation, etc.) ;
- Déconnectez la machine du réseau, pour stopper l'attaque. En revanche, maintenez-là sous tension et ne la redémarrez pas, pour ne pas perdre d'informations utiles pour l'analyse de l'attaque ;
- Prévenez votre hiérarchie, ainsi que le responsable de la sécurité, au téléphone ou de vive voix, car l'intrus peut être capable de lire les courriels. Prenez également contact avec un prestataire informatique qui vous aidera dans la restauration de votre système ainsi que dans l'analyse de l'attaque ;
- Faites faire une copie physique du disque ;
- Faites rechercher les traces disponibles liées à la compromission. Un équipement n'étant jamais isolé dans un système d'information, des traces de sa compromission doivent exister dans d'autres équipements sur le réseau (pare-feu, routeurs, outils de détection d'intrusion, etc.). Vous pouvez faire appel à une société spécialisée.
- Déposez une plainte auprès de la brigade de gendarmerie ou du service de police judiciaire compétent pour le siège de la société, de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (Paris et petite couronne), ou de la Direction générale de la sécurité intérieure. Retrouvez plus d'informations sur le site de l'ANSSI : www.ssi.gouv.fr/en-cas-dincident/ ;
- Après l'incident : réinstallez complètement le système d'exploitation à partir d'une version saine, supprimez tous les services inutiles, restaurez les données d'après une copie de sauvegarde non compromise, et changez tous les mots de passe du système d'information.

CHECKLIST

Soupçon d'intrusion

- ☐ Déconnectez la machine du réseau
- ☐ Maintenir sous tension
- ☐ Ne pas redémarrez
- ☐ Prévenez votre hiérarchie,
- ☐ Prenez également contact avec un prestataire informatique pour restaurer votre système
- ☐ Faites faire une copie physique du disque
- ☐ Rechercher les traces de compromission du système d'information
- ☐ Déposez une plainte : Voir FICHE R1 « ***Prévenir les autorités*** »

Après l'incident

- ☐ Réinstallez complètement le système d'exploitation
- ☐ Supprimez tous les services inutiles
- ☐ Restaurez les données d'après une copie de sauvegarde

Liens utiles

Menaces et bonnes pratiques | cybermalveillance.gouv.fr
Sécuriser un site web | ANSSI ssi.gouv.fr
Bonnes pratiques pour les entreprises | ANSSI ssi.gouv.fr
Bonnes pratiques pour les administrations | ANSSI ssi.gouv.fr
Formation en ligne à la sécurité du numérique – MOOC | ANSSI secnuacademie.gouv.fr

FICHE PROCÉDURALE

R7

RÉACTION | SIGNALEMENT D'UN INDIVIDU SUSPECT

Chacun 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.

Pourquoi signaler une situation suspecte ?

En étant attentif à son environnement quotidien, chacun peut remarquer et signaler des faits, objets ou comportement 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.

La préparation d'un attentat peut être simple ou complexe :

- **Attentat simple :** L'individu pourra être détecté juste avant son passage à l'acte ;
- **Attentat complexe :** Des indices de sa préparation et des moyens humains et matériels pourront être repérés.

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

Comment détecter une situation suspecte ?

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 apprendre à être un observateur attentif de son environnement.

Un individu sur le point de commettre un attentat manifestera un comportement pouvant trancher avec son environnement : signe de peur, d'anxiété ou de dissimulation. Plusieurs individus peuvent également se préparer ensemble à passer à l'acte et avoir un comportement coordonné.

Faites appel à votre bon sens et votre intuition

Préparation

Les terroristes conduisent souvent 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. Vous pouvez donc être vigilant si vous observez :

- Stationnement prolongé d'un véhicule à proximité du lieu de rassemblement sans raison apparente.
- Stationnement prolongé d'un véhicule sans plaque d'immatriculation.
- Demande de renseignements sur les mesures de sécurité par le biais de discussions en apparences anodines.
- Prises de vue des infrastructures du site ciblé et du dispositif de protection mis en place.
- Observation de la manière dont se déroulent les contrôles de sécurité

Action

Un individu sur le point de commettre une attaque terroriste dissimulera probablement des armes de quelque nature que ce soit. Il aura par conséquent une tenue adaptée et pourra :

- Porter un sac anormalement lourd ou déformé par une arme
- Porter des protections
- Avoir une tenue inappropriée pour la saison (vêtement ample pouvant dissimuler une arme)
- Montrer des signes de nervosité, de colère, d'anxiété ou de méfiance en contraste avec l'environnement

Certaines situations doivent aussi vous alerter : Un colis ou un sac abandonné, un sac positionné dans un lieu de passage important.

Comment réagir et signaler ?

Si vous être témoin d'un comportement suspect, **restez discret.** Des procédures internes doivent permettre la remontée très rapide d'un signalement. Observez et mémorisez des éléments objectifs qui pourraient être transmis à la police ou à la gendarmerie nationales (plaque d'immatriculation, modèle de véhicule, description précise des individus, direction de fuite, etc.).

Vous pouvez **engager une conversation** normale avec l'individu dont le comportement a été remarqué (questions ouvertes pouvant m'aider à déterminer si l'individu repéré par son comportement dissimule de mauvaises intentions).

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 et à parler).

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

Incohérence → étonnement → signalement

Comprendre la manière dont se planifie une action violente peut vous aider à déceler certains indices de préparation

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 indifférenciées (population dans son ensemble) pour créer un climat de terreur et/ou toucher les intérêts économiques du pays.

La préparation de l'action

Les terroristes conduisent souvent 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 (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, ou observation du déroulement des contrôles de sécurité ;
  - 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.).

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-balle) ;
- 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, de colère, d'anxiété 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 depuis longtemps à proximité d'un lieu de rassemblement (marché, lieu de culte, etc.) ou d'un site sensible (mairie, ambassade, etc.).

CHECKLIST

Questions	Réponse			Remarques
	O	N	SO	(Description)
Un véhicule est-il stationné de façon prolongée ?				
Le véhicule est-il à proximité d'un lieu de rassemblement sans raison apparente ?				
Un individu a-t-il demandé des renseignements sur les mesures de sécurité par le biais de discussions en apparences anodines ?				
Des prises de vue des infrastructures du site ciblé et du dispositif de protection mis en place ont elles recensées ?				
Un individu porte-t-il un sac anormalement lourd ou déformé ?				
Un individu porte-t-il une tenue inappropriée (saison, protections) ?				
Un individu présente-t-il des signes de méfiance, de colère, d'anxiété ou de nervosité ?				

Réagir

- ☐ Restez discret
- ☐ Observez et mémorisez des éléments objectifs
- ☐ Plaque d'immatriculation : . . . . . .
- ☐ Modèle de véhicule :. . . . . .
- ☐ Description précise des individus : . . . . . .
- ☐ Direction de fuite : . . . . . .
- ☐ Engager une conversation normale avec l'individu

CHECKLIST

Alerter

☐ Rendre compte au responsable du site

☐ Alerter les services de police ou de gendarmerie (17). Voir FICHE R1 « ***Prévenir les autorités*** »

Arrivée des secours

☐ Signaler auprès des services de secours tout élément susceptible d'entraîner un risque

☐ Suivre à la lettre les instructions qui sont données par les services de secours

Liens utiles

Stop Djihadisme | gouvernement.fr

Signalement de situations suspectes – Recommandation à l'usage du public | sgdsn.gouv.fr

Prévention et signalement des cas de radicalisation djihadiste | sgdsn.gouv.fr

Réagir en cas d'attaque terroriste – Alerter | sgdsn.gouv.fr

Fiche message d'alerte - Guide d'aide à l'élaboration d'un PSE - p. 37 | solidarites-sante.gouv.fr

FICHE PROCÉDURALE

R8

RÉACTION | FOUILLE DES LOCAUX

Il s'agit de mettre à l'abri l'ensemble des visiteurs et le personnel de l'établissement en respectant par défaut les distances suivantes :

Rayon d'évacuation :

- Engin explosif improvisé (IED) : 100 m à couvert ;
- Véhicule : 200 m à couvert.

Les forces de sécurité intérieure et/ou les démineurs peuvent décider à tout moment de modifier les conditions d'évacuation décrites ci-après en fonction de la nature de la menace.

Heure d'explosion / Lieu d'explosion	DÉTERMINÉ	INDÉTERMINÉE
DÉTERMINÉE	• Évacuation immédiate • Fouille immédiate de l'endroit désigné • Stopper les fouilles **30 mn avant et après** l'heure prévue d'explosion	• Évacuation immédiate • Fouille immédiate sans interruption dans le temps
INDÉTERMINÉE	• Évacuation immédiate • Fouille immédiate de toute l'installation • Stopper les fouilles **30 mn avant et après** l'heure prévue d'explosion	• Pas d'évacuation • Fouille immédiate

Décision d'évacuation :

- Directeur de l'établissement ;
- Responsable de l'ordre public s'il y a danger imminent ou si la voie publique est concernée.

Modalités d'évacuation pour les personnes évacuées :

1. Examiner la pièce à évacuer :

- Aucun objet suspect → marque sur la porte signalant l'inspection négative ;
- Objet suspect → mémoriser l'emplacement et le signaler au responsable des fouilles. Accélérer l'évacuation.

2. Emporter tous les effets personnels (afin de ne pas multiplier le nombre d'objets abandonnés).

MOYENS

M1 | Mise en place d'un système de vidéosurveillance 101
M2 | Mise en place d'un système de contrôle des accès 107
M3 | Mesures d'entraves aux véhicules béliers . . 110
M4 | Mise à niveau de la sécurité des systèmes d'informations 112

FICHE PROCÉDURALE

M1 MOYENS | MISE EN PLACE D'UN SYSTÈME DE VIDÉOSURVEILLANCE

Les recommandations figurant dans cette fiche sont à adapter en fonction du lieu, de la nature, de l'importance et de la durée de l'événement auquel elles peuvent s'appliquer.

Les systèmes de vidéoprotection peuvent contribuer de plusieurs façons à la prévention et à la lutte contre le terrorisme. De façon préventive, les caméras peuvent permettre de détecter des éléments suspects, d'estimer si une alerte est réelle ou non et d'aider à la prise de décisions par le directeur ou responsable sûreté du site. D'un point de vue répressif, après un incident, les enregistrements des caméras pourront fournir des renseignements particulièrement utiles aux enquêteurs sur le mode opérateur des agresseurs mais aussi contribuer à leur identification.

Cadre juridique applicable

Il va dépendre de la nature des lieux qui seront filmés :

- **Dans les parties privatives non accessibles au public** (coulisses, réserves, zones dédiées au personnel, etc.) : l'installation de caméra, pour filmer et enregistrer ces locaux, pourra être soumise à une déclaration à la CNIL (conformément aux dispositions de la loi 78-17 du 6 janvier 78), si la/les personne(s) qui accède(nt) aux enregistrements peut/peuvent identifier une part significative des personnes qui fréquentent ces locaux. Dans la négative aucune déclaration n'est nécessaire (cf. circulaire du Premier ministre PRMX1124533C du 14/09/11).

  Ces locaux étant souvent soumis aux dispositions du code du travail, l'employeur devra toutefois respecter les articles L 1221-9, L 1222-4 et L 2323-32. Il devra donc informer le personnel individuellement de l'installation des caméras et, si un comité d'entreprise existe, il doit être informé et consulté préalablement à toute installation.

  — La CNIL considère que la durée de conservation de ces images ne doit pas dépasser 1 mois. —

- **Dans les parties accueillant du public** (lieux et établissements ouverts au public) : l'installation de caméras pour visualiser et /ou enregistrer ces lieux, aux fins d'y assurer la sécurité des personnes et des biens lorsque ces lieux et établissements sont particulièrement exposés à des risques d'agression ou de vol, est soumise à une autorisation préalable délivrée par le préfet de département, après avis de la commission départementale de vidéoprotection, conformément aux articles L.251-1 à L.255-1 et R.251-1 à R.253-4 du code de la sécurité intérieure (CSI).

L'autorisation est valable 5 ans maximum, renouvelable. La durée de conservation des images est fixée par l'autorisation préfectorale, elle ne peut dépasser un mois (hors réquisition des services de police ou de justice). Une durée minimale de conservation peut être prescrite. Le public doit être informé de manière claire et permanente de l'existence du système de vidéoprotection et de l'autorité ou

de la personne responsable. Un droit d'accès aux enregistrements la concernant est reconnu à toute personne intéressée. Un refus n'est possible que pour un motif tenant à la sûreté de l'État, à la défense, à la sécurité publique, au déroulement de procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures ou au droit des tiers.

Si le lieu de travail est ouvert au public, les dispositions du CSI et du code du travail s'appliquent de façon cumulative.

- **Sur la voie publique :** la transmission et l'enregistrement d'images prises par le moyen de la vidéoprotection ne peuvent être mis en œuvre que par les autorités publiques dans le cadre de 9 finalités, sur la base d'une autorisation préalable délivrée par le préfet de département, après avis de la commission départementale de vidéoprotection.

  Les opérations de vidéoprotection de la voie publique sont réalisées de telle sorte qu'elles ne visualisent pas les images de l'intérieur des immeubles d'habitation ni, de façon spécifique, celles de leurs entrées.

L'autorisation est valable 5 ans maximum, renouvelable. La durée de conservation des images est fixée par l'autorisation préfectorale, elle ne peut dépasser un mois (hors réquisition des services de police ou de justice). Une durée minimale de conservation peut être prescrite. Le public doit être informé de manière claire et permanente de l'existence du système de vidéoprotection et de l'autorité responsable. Un droit d'accès aux enregistrements la concernant est reconnu à toute personne intéressée. Un refus n'est possible que pour un motif tenant à la sûreté de l'État, à la défense, à la sécurité publique, au déroulement de procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures ou au droit des tiers.

N.B. si un secteur de voie publique est privatisé pour y organiser un festival par exemple, les organisateurs pourront se voir autoriser à y installer des caméras et pourront les visionner comme pour un lieu ouvert au public.

Cas particulier du risque terroriste

Les personnes morales publiques ou privées (non autorités publiques) peuvent être autorisées par le préfet du département à mettre en place des caméras pour visionner et enregistrer la voie publique, pour la protection des abords immédiats de leurs bâtiments et installations, dans les lieux susceptibles d'être exposés à des actes de terrorisme.

Il peut être également procédé à ces opérations (d'enregistrement et de transmission d'images) dans des lieux et établissements ouverts au public (à l'intérieur des locaux) aux fins d'y assurer la sécurité des personnes et des biens lorsque ces lieux et établissements sont susceptibles d'être exposés à des actes de terrorisme. Cf. art L 223-1 du CSI.

L'autorisation est valable 5 ans maximum, renouvelable. La durée de conservation des images est fixée par l'autorisation préfectorale, elle ne peut dépasser un mois (hors réquisition des services de police

ou de justice). Une durée minimale de conservation peut être prescrite. Le public doit être informé de manière claire et permanente de l'existence du système de vidéoprotection et de l'autorité ou de la personne responsable. Un droit d'accès aux enregistrements la concernant est reconnu à toute personne intéressée. Un refus n'est possible que pour un motif tenant à la sûreté de l'État, à la défense, à la sécurité publique, au déroulement de procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures ou au droit des tiers.

L'article L 223-4 du CSI permet au préfet du département lorsque l'urgence et l'exposition particulière à un risque d'actes de terrorisme le requièrent d'autoriser provisoirement (pour une durée de 4 mois maxi), sans avis préalable de la commission départementale de vidéoprotection, les personnes mentionnées à l'article L. 223-1, à installer un dispositif de vidéoprotection.

L'article L 223-5 du CSI autorise le préfet du département lorsque l'urgence et l'exposition particulière à un risque d'actes de terrorisme le requièrent à prescrire la mise en œuvre d'un système de vidéoprotection.

N.B. tous les dispositifs soumis à autorisation préfectorale doivent répondre à des normes techniques minimum actuellement fixées par l'arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéoprotection N° NOR : IOCD0762353A.

ATTENTION - Dispositifs nécessitant une autorisation de la CNIL : Dans tous les cas de figure (lieux privés, lieux publics, voie publique, terrorisme), les systèmes de vidéoprotection dont les enregistrements sont intégrés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier par eux-mêmes, directement ou indirectement des personnes physiques du fait des fonctionnalités qu'ils comportent, doivent être autorisés par la CNIL.

Le contrôle des dispositifs de vidéoprotection

Les représentants de la commission départementale de vidéoprotection (pour les caméras soumises à autorisation préfectorales), de la commission nationale de l'informatique et des libertés (pour tous les dispositifs) peuvent effectuer des contrôles des dispositifs de vidéoprotection, entre 6h et 21h. Le responsable du site peut s'opposer à cette visite. Celle-ci ne pourra alors se faire qu'avec l'autorisation du juge des libertés et de la détention du tribunal de grande instance territorialement compétent (art. L 253-3 du CSI).

Les représentants des forces de sécurité de l'État peuvent aussi contrôler les conditions de mises en œuvre de tous les dispositifs dans un cadre de police administrative. Aucune opposition n'est possible dans ce cas.

Durée d'enregistrement

Dans tous les cas de figure, que l'on cherche à se prémunir contre des actes de délinquance ordinaire ou de terrorisme, il est préférable de solliciter ou de prévoir la plus grande durée d'enregistrement possible. En effet, ces actes sont souvent précédés de repérages préalables par leurs auteurs. L'examen des images des jours précédant les faits permet donc aux enquêteurs de récupérer des éléments utiles aux enquêtes en cours. La durée de conservation minimum souhaitable est de 10 à 15 jours.

Le visionnage des images

Si vous mettez en place un dispositif de vidéoprotection dans un but préventif et particulièrement si vous avez demandé à pouvoir visualiser les abords immédiats de votre site pour lutter contre le terrorisme, vous devez en assurer le visionnage. La seule présence d'un enregistrement étant, dans ce cas, insuffisante.

Pour cela vous devrez charger un ou plusieurs de vos employés (appartenant éventuellement à votre service interne de sécurité si vous en disposez) du visionnage des images. Vous pouvez aussi décider de confier cette tâche à une entreprise de sécurité privée dont les employés devront être agréés par le CNAPS.

Dans l'idéal les caméras devront être surveillées en permanence et a minima sur la période de présence du public, en prévoyant une marge suffisante pour couvrir les phases d'arrivée et de départ des spectateurs et ce tout particulièrement si vous avez obtenu la visualisation des abords de votre site.

Pour assurer une utilisation optimum de cette veille proactive il convient :

- Que les caméras couvrent l'ensemble des entrées et des sorties du site, les lieux de rassemblement du public, ainsi que d'autres secteurs essentiels à la gestion et à la sécurité de votre activité ;
- Que l'opérateur cherche à détecter les comportements « anormaux » par rapport aux attitudes générales propres aux différents publics attendus ;
- Si la caméra dispose d'une fonction zoom, de l'utiliser pour faire un gros plan des personnes ainsi repérées afin de permettre leur éventuelle identification par la suite ;
- De signaler les personnes repérées aux éventuels agents de sécurité ou représentants des forces de l'ordre présents sur place.

Si le reste du temps les caméras ne sont pas surveillées, il convient d'effectuer régulièrement une visualisation des enregistrements pour vérifier d'une part le bon fonctionnement du dispositif et d'autre part qu'aucun événement suspect ne s'est produit.

Comment évaluer son dispositif ?

Posez-vous les questions suivantes :

- Votre système de vidéoprotection permet-il actuellement de réaliser ce que vous exigez de lui ? Vous apporte-t-il la couverture vidéo nécessaire ou subsiste-t-il des zones à risques non couvertes ? Dans ce cas il convient de rajouter des caméras ou de mettre en place des procédures pour pallier ce déficit ;
- La qualité des images obtenues permet-elle une identification possible des personnes présentes ou des véhicules ou seulement leur détection ?
- La qualité des images est-elle constante et conforme à vos attentes, quelles que soient les conditions de luminosité (jour/ nuit, éclairage interne maximum / éclairage interne minimum). Dans la négative, il peut être nécessaire de prévoir un éclairage d'appoint (ou infrarouge) ou d'installer des caméras ayant besoin de moins de luminosité pour bien fonctionner ;
- La qualité des images est-elle constante quelles que soient les conditions climatiques (pluie, neige, brouillard, températures élevées ou négatives, etc.) ? Dans la négative : prévoir des caissons thermostatés, revoir les réglages, etc. ;
- La qualité des images est-elle identique en direct et sur les enregistrements ? S'il y a une trop grande disparité liée souvent au taux de compression utilisé, les possibilités d'utilisation des images comme éléments probatoires pourront être remis en cause ;
- L'horodatage du système est-il exact ? Dans la négative le faire régler le plus rapidement possible, sinon là aussi les images ne pourront être retenues comme élément probant ;
- La maintenance du système est-elle prévue ? Est-elle interne ou bien effectuée par un prestataire extérieur ? Les délais et fréquences d'intervention sont-ils suffisants ?

Organisation du poste de visionnage

- Le lieu doit être installé dans une pièce protégée à l'intérieur du site et non directement à l'entrée. D'autant plus si les enregistrements y sont également stockés.
- Il doit être doté de moyen de communication vers l'extérieur (téléphone) et intérieur (radio, interphone, etc.).
- Il convient de tenir compte du nombre maximum d'images vidéo qu'un seul opérateur peut efficacement surveiller simultanément (6/8 grand maximum).
- Pour permettre de détecter des faits ou des comportements il convient également que les images à surveiller ne soient pas trop petites, un écran d'ordinateur classique ne doit ainsi pas afficher plus de 4 images.
- Tenez compte de la concentration nécessaire pour faire une veille active, un même opérateur ne pourra pas rester concentré sur les images plusieurs heures de façon ininterrompue.
- Il est judicieux de concevoir l'installation du poste de visionnage dans le Poste Central de Sûreté.
- Éventuellement, conditionner l'affichage des images à de la détection ou du contrôle d'accès.

Vérification du système de vidéosurveillance

Questions	Réponse			Remarques
	O	N	SO	(Description et influence sur les risques du site)
Des caméras extérieures surveillent-elles les façades et les accès ?				
Des caméras intérieures couvrent-elles les accès au bâtiment et les locaux sensibles du site ?				
Les caméras sont-elles actives en permanence ? (Pendant et hors périodes d'activité)				
Les images sont-elles visualisables en direct par le responsable de la sûreté du site ?				
Les images sont-elles enregistrées sur le site ? Si oui, quelle est la durée de conservation ?				
Les images sont-elles reportées à un service de télésurveillance ?				

Liens utiles

Gérer la sûreté et la sécurité des évènements et sites culturels | culture.gouv.fr

Référent sûreté | referentsurete.fr

FICHE PROCÉDURALE

M2 MOYENS | MISE EN PLACE D'UN SYSTÈME DE CONTRÔLE DES ACCÈS

Tout manque de vigilance aux abords des entrées d'une manifestation ou à l'égard des files d'attente offre l'anonymat à un éventuel terroriste.

Le personnel de sécurité déployé à l'extérieur doit adopter le principe « voir et être vu » et, dans la mesure du possible, maintenir l'ordre dans les files d'attente au-dehors de la manifestation. La file d'attente doit être bien ordonnée, surveillée par les opérateurs du système de vidéosurveillance le cas échéant, et la communication entre les visiteurs et le personnel établie.

Autant que possible, privilégiez une gestion de file d'attente entre l'espace public et le site de l'événement.

Ceci est particulièrement important si l'on prévoit de longues files d'attente à l'entrée d'une manifestation. L'objectif étant de limiter la longueur des files et la durée de l'attente.

Envisagez d'organiser le processus de file d'attente de manière à permettre au personnel de sécurité d'examiner minutieusement chaque visiteur au moment où il pénètre sur le site de la manifestation. Le personnel doit être informé de ce qu'il doit rechercher et des procédures à suivre dans chaque situation.

Au sein du site réservé à l'événement, la démarcation entre les espaces publics et privés doit être clairement visible, et des mesures appropriées de contrôle d'accès à l'entrée et à la sortie de la partie privée doivent être mises en place.

Définissez le niveau de sécurité requis avant de planifier votre système de contrôle d'accès.

Accessibilité

Examiner l'organisation de votre système. Assurez-vous que vos procédures d'entrée et de sortie permettent aux usagers autorisés de passer sans efforts ni retards excessifs. Inspirez-vous si possible des systèmes électroniques de billetterie.

Dans l'idéal, pour les personnels affectés à l'événement, adoptez un système de contrôle d'accès basé sur une identification avec photo, dont l'aspect varie selon les différents niveaux d'accès appliqués sur le site. Le personnel de sûreté doit être informé des éléments à examiner lors du contrôle des badges : la qualité dudit contrôle doit être vérifiée par une mise à l'épreuve.

Formation

Assurez-vous que votre personnel ait pleinement connaissance du rôle et du fonctionnement de votre système de contrôle d'accès. Votre installateur doit assurer une formation adéquate à cet égard.

Maintenance du système

Si vous disposez de portiques de détection ou de magnétomètres, votre installateur doit fournir toute la documentation pertinente relative à votre système (registres, calendriers d'entretien, etc..

- Connaissez-vous les mesures à prendre en cas de panne du système ?
- Votre système est-il couvert par un contrat de maintenance satisfaisant ?
- Existe-t-il un plan que vous pouvez mettre en œuvre au pied levé ?

Vérification du système de contrôle des accès

Questions	Réponse			Remarques
	O	N	SO	(Description et influence sur les risques du site)
Le contrôle d'accès des locaux est-il assuré par : • ***Un verrouillage par serrure ?*** • ***Un interphone/visiophone avec ouverture de porte ?*** • ***Une serrure à code mécanique ?*** • ***Un lecteur de badge/carte ?*** • ***Autre ?***				
L'ensemble des portes d'entrée au bâtiment ainsi que celles des locaux considérés comme sensibles sont-ils sous contrôle d'accès ?				
Existe-t-il des droits d'accès différents en fonction des différents profils de personnels ?				
En cas de porte sous contrôle d'accès forcée ou maintenue ouverte, existe-t-il un report d'alarme ?				

A quel endroit (sur site ou à distance) ?				
En cas d'intervention sur téléalarme, l'agent intervenant dispose-t-il des droits et badge d'accès ?				
Existe-t-il des plages horaires d'activation des systèmes de contrôle d'accès et/ou de détection intrusion ?				
Des détecteurs d'intrusion surveillent-ils les fenêtres et les portes d'accès du bâtiment ?				
Si oui, ces détecteurs sont-ils reliés à des équipements de sûreté (sirène, éclairage, caméra) ?				
Des détecteurs d'intrusion couvrent-ils les locaux sensibles du site ?				
Les détecteurs d'intrusion sont-ils actifs en permanence ? (Pendant et hors périodes d'activité)				
En cas d'intrusion, une alarme est-elle transmise au responsable de la sûreté du site ?				
Un contrat de télésurveillance avec report des alarmes en cas de détection existe-t-il ?				
En cas d'intrusion, le service de télésurveillance envoie-t-il un agent de sûreté faire une levée de doute ?				

Liens utiles

Gérer la sûreté et la sécurité des évènements et sites culturels | culture.gouv.fr

FICHE PROCÉDURALE

M3

MOYENS | MESURES D'ENTRAVES AUX VÉHICULES BÉLIERS

Cette fiche réflexe présente les bonnes pratiques en matière de protection d'un évènement de voie publique contre les attaques au véhicule bélier. Ce document, à vocation opérationnelle, doit pouvoir guider l'organisateur dans la préparation de ce genre de manifestation.

Identifier les menaces et les vulnérabilités

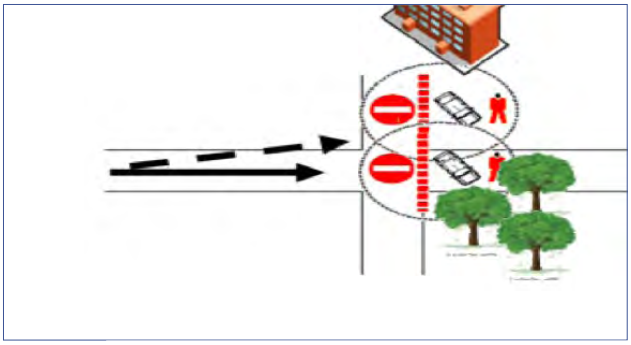
Objectif opérationnel : Se prémunir des attaques au véhicule bélier par un plan cohérent de circulation et d'interdiction des véhicules.

Chaque véhicule peut potentiellement présenter une menace pour la sécurité de l'événement. Outre son utilisation en véhicule bélier, quelle que soit sa taille, il peut également transporter et contenir une charge d'explosifs non négligeable.

Le contrôle de véhicule est donc indispensable avant son accès au site de l'événement.
Le parking véhicule doit impérativement être installé à l'extérieur du site de l'événement.

- **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 ?

- **Réfléchir en amont à un plan cohérent de circulation routière :**
  - Choisir le lieu d'implantation de l'événement qui présentera le moins de vulnérabilités – s'appuyer notamment sur la configuration naturelle du terrain (cours d'eau fossés, talus, zones boisées, etc.) ;
  - Identifier les points clefs et/ ou de vulnérabilités du réseau routier (carrefour, rond-point, axe de circulation, etc.) ;
  - Limiter ou interdire le stationnement des véhicules aux abords immédiats du lieu de rassemblement ;



Exemple de plan de circulation

- Cloisonner les flux des véhicules de l'espace de déambulation des piétons ;
- À l'aide d'une signalisation récurrente et adaptée, procéder par zonage = zone parking, zone d'accès, zone piétonne, etc.

Organiser la sécurité de l'événement

En lien avec les autorités locales (préfet, maire, police nationale, gendarmerie nationale) mettre en place un plan global de circulation routière, afin de fluidifier les accès – cloisonner les flux entrants / sortant, faciliter l'intervention des secours et ralentir la vitesse aux abords du lieu de l'événement.

Afin de mettre en œuvre les moyens physiques dédiés, vous aurez besoin :

- D'un **permis de stationnement** autorisation l'occupation sans emprise au sol. Attention : Si le chantier impacte la circulation publique, la demande doit être complétée par une demande d'arrêté de circulation.

ET / OU

- D'une **permission de voirie** autorisant l'occupation avec emprise sur le sol et pour des travaux modifiant le domaine public. Attention : Si le chantier de mise en place de ces moyens impacte la circulation publique, la demande doit être complétée par une demande d'arrêté de circulation.

ET / OU

- D'un **arrêté de circulation** si interruption ou modification de la circulation. Il est nécessaire d'en obtenir l'autorisation par un arrêté temporaire de police de circulation, préalable à la police de circulation, préalable à la mise en place d'une signalisation spécifique.

Liens utiles

Se protéger contre les attaques aux véhicules béliers | sgdsn.gouv.fr

FICHE PROCÉDURALE

M4

MOYENS | MISE À NIVEAU DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATIONS

Alors que le numérique fait désormais partie intégrante de nos vies personnelles et professionnelles, la sécurité est trop rarement prise en compte dans nos usages. Les nouvelles technologies, omniprésentes, sont pourtant porteuses de nouveaux risques pesant lourdement sur les espaces publics. Par exemple, les données les plus sensibles (fichiers clients, contrats, projets en cours, etc.) peuvent être dérobées par des attaquants informatiques ou récupérées en cas de perte ou vol d'un smartphone, d'une tablette, d'un ordinateur portable. Ces incidents s'accompagnent souvent de sévères répercussions en termes de sécurité, de pertes économiques et financières et de dégradations. Ces dangers peuvent néanmoins être fortement réduits par un ensemble de bonnes pratiques, peu coûteuses, voire gratuites, et faciles à mettre en œuvre. À cet effet, la sensibilisation des collaborateurs aux règles d'hygiène informatique est fondamentale et surtout très efficace pour limiter une grande partie des risques.

Choisir avec soin ses mots de passe

Pour bien protéger vos informations, choisissez des mots de passe difficiles à retrouver à l'aide d'outils automatisés ou à deviner par une tierce personne. Choisissez des mots de passe composés si possible de 12 caractères de type différents (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien avec vous (nom, date de naissance, etc.) et ne figurant pas dans le dictionnaire. Définissez un mot de passe unique pour chaque service sensible. Les mots de passe protégeant des contenus sensibles (banque, messagerie professionnelle, etc.) ne doivent jamais être réutilisés pour d'autres services.

Mettre à jour régulièrement vos logiciels

Dans chaque système d'exploitation (Android, IOS, MacOS, Linux, Windows, etc.), logiciel ou application, des vulnérabilités existent. Une fois découvertes, elles sont corrigées par les éditeurs qui proposent alors aux utilisateurs des mises à jour de sécurité. Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les attaquants exploitent ces vulnérabilités pour mener à bien leurs opérations encore longtemps après leur découverte et leur correction. Il convient donc de configurer vos logiciels pour que les mises à jour de sécurité s'installent automatiquement ou d'utiliser exclusivement les sites internet officiels des opérateurs.

Bien connaître ses utilisateurs et ses prestataires

Lorsque vous accédez à votre ordinateur, vous bénéficiez de droits d'utilisation plus ou moins élevés sur celui-ci. On distingue généralement les droits dits « d'utilisateur » et les droits dits « d'administrateur ». Dans l'utilisation quotidienne de votre ordinateur (naviguer sur Internet, lire ses courriels, utiliser des logiciels de bureautique, de jeu, etc.), prenez un compte utilisateur : il répondra parfaitement à vos besoins. Le compte administrateur n'est à utiliser que pour intervenir sur le fonctionnement global de l'ordinateur (gérer des comptes utilisateurs, modifier la politique de sécurité, installer ou mettre à jour des logiciels, etc.).

Il convient donc de :

- Réserver l'utilisation du profil « administrateur » au service informatique, si celui-ci existe ;
- Dans le cas contraire, protéger en l'accès : n'ouvrez pour les employés que des comptes utilisateur, n'utilisez pas le compte administrateur pour de la navigation sur Internet ;
- Identifier précisément les différents utilisateurs du système et les privilèges qui leur sont accordés. Tous ne peuvent pas bénéficier de droits d'administrateur ;
- Supprimer les comptes anonymes et génériques (stagiaire, contact, presse, etc.). Chaque utilisateur doit être identifié nommément afin de pouvoir relier une action sur le système à un utilisateur ;
- Encadrer par des procédures déterminées les arrivées et les départs de personnel pour vous assurer que les droits octroyés sur les systèmes d'information sont appliqués au plus juste et surtout qu'ils sont révoqués lors du départ de la personne.

Effectuer des sauvegardes régulières

Pour veiller à la sécurité de vos données, il est vivement conseillé d'effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires par exemple). Vous pourrez alors en disposer suite à un dysfonctionnement de votre système d'exploitation ou à une attaque.

Pour sauvegarder vos données, vous pouvez utiliser des supports externes tels qu'un disque dur externe réservé exclusivement à cet usage, ou, à défaut, un CD ou un DVD enregistrable que vous rangerez ensuite dans un lieu éloigné de votre ordinateur, de préférence à l'extérieur de l'entreprise pour éviter que la destruction des données d'origine ne s'accompagne de la destruction de la copie de sauvegarde en cas d'incendie ou d'inondation ou que la copie de sauvegarde ne soit volée en même temps que l'ordinateur contenant les données d'origine. Néanmoins, il est nécessaire d'accorder une attention particulière à la durée de vie de ces supports.

Sécuriser l'accès Wi-Fi de votre espace public

L'utilisation du Wi-Fi est une pratique attractive. Il ne faut cependant pas oublier qu'un Wi-Fi mal sécurisé peut permettre à des personnes d'intercepter vos données et d'utiliser la connexion Wi-Fi à votre insu pour réaliser des opérations malveillantes. Pour cette raison l'accès à Internet par un point d'accès Wi-Fi est à éviter dans le cadre de l'entreprise : une installation filaire reste plus sécurisée et plus performante.

Le Wi-Fi peut parfois être le seul moyen possible d'accéder à Internet, il convient dans ce cas de sécuriser l'accès en configurant votre borne d'accès à Internet. Pour ce faire, n'hésitez pas à contacter l'assistance technique de votre fournisseur d'accès. Ce dernier pourra vous guider dans cette configuration en vous proposant différentes étapes pour sécuriser votre réseau.

Par ailleurs, n'utilisez pas les Wi-Fi « publics » (réseaux offerts dans les gares, les aéroports ou les hôtels) pour des raisons de sécurité et de confidentialité. Assurez-vous également que votre ordinateur est bien protégé par un antivirus et un pare-feu.

Être prudent lors de l'utilisation de sa messagerie

Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées, etc.).

Lorsque vous recevez des courriels, prenez les précautions suivantes :

- L'identité d'un expéditeur n'étant en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message et vérifiez son identité. En cas de doute, ne pas hésiter à contacter directement l'émetteur du mail par téléphone ;
- N'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts ;
- Si des liens figurent dans un courriel, passez votre souris dessus avant de cliquer. L'adresse complète du site s'affichera dans la barre d'état du navigateur située en bas à gauche de la fenêtre (à condition de l'avoir préalablement activée). Vous pourrez ainsi en vérifier la cohérence ;
- Ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire). En effet, des courriels circulent aux couleurs d'institutions comme les impôts pour récupérer vos données. Il s'agit d'attaques par hameçonnage ou « phishing » ;
- Désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue.

Télécharger ses programmes sur les sites officiels des éditeurs

Si vous téléchargez du contenu numérique sur des sites Internet dont la confiance n'est pas assurée, vous prenez le risque d'enregistrer sur votre ordinateur des programmes ne pouvant être mis à jour, qui, le plus souvent, contiennent des virus ou des chevaux de Troie. Cela peut permettre à des personnes malveillantes de prendre le contrôle à distance de votre machine pour espionner les actions réalisées sur votre ordinateur, voler vos données personnelles, lancer des attaques, etc.

Il convient donc de téléchargez vos programmes sur les sites de leurs éditeurs ou d'autres sites de confiance, de rester vigilants concernant les liens sponsorisés et de désactiver l'ouverture automatique des documents sans avoir lancé une analyse antivirus préalable.

CHECKLIST

Choisir avec soin ses mots de passe

Mon mot de passe contient :

12 caractères minimum

☐ Oui ☐ Non, combien ? .....

Des majuscules

☐ Oui ☐ Non

Des minuscules

☐ Oui ☐ Non

Des chiffres

☐ Oui ☐ Non

Des caractères spéciaux

☐ Oui ☐ Non

Mon mot de passe ne contient aucun élément personnel

☐ Oui ☐ Non

Mon mot de passe contient des mots du dictionnaire

☐ Oui ☐ Non

Mes logiciels sont à jours

☐ Oui ☐ Non, pourquoi ? .....

CHECKLIST

Bien connaître ses utilisateurs et ses prestataires

- ☐ Réserver l'utilisation du profil « administrateur » au service informatique
- ☐ N'ouvrez pour les employés que des comptes utilisateur
- ☐ N'utilisez pas le compte administrateur pour de la navigation sur Internet
- ☐ Identifier précisément les différents utilisateurs du système et les privilèges qui leur sont accordés
- ☐ Supprimer les comptes anonymes et génériques
- ☐ Encadrer par des procédures déterminées les arrivées et les départs de personnel
- ☐ Effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires)
- ☐ Sécuriser l'accès Wi-Fi de votre espace public

Sécurisez vos courriels

- ☐ Vérifiez la cohérence entre l'expéditeur présumé et le contenu du message
- ☐ N'ouvrez pas les pièces jointes provenant de destinataires inconnus
- ☐ Ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles
- ☐ Désactivez l'ouverture automatique des documents téléchargés

Liens utiles

Guide des bonnes pratiques de l'informatique | ANSSI ssi.gouv.fr

Sécuriser un site web | ANSSI ssi.gouv.fr

Bonnes pratiques pour les entreprises | ANSSI ssi.gouv.fr

Bonnes pratiques pour les administrations | ANSSI ssi.gouv.fr

Formation en ligne à la sécurité du numérique – MOOC | ANSSI secnuacademie.gouv.fr

POUR ALLER PLUS LOIN

Contacts utiles

SGDSN | sgdsn.gouv.fr

Par courrier postal :

Secrétariat général de la défense et de la sécurité nationale
51 boulevard de la Tour-Maubourg
75700 Paris 07 SP

Par courrier électronique | courrier.sgdsn@sgdsn.gouv.fr

Liens utiles

Formation à la vigilance, la prévention et la protection face à la menace terroriste MOOC | SGDSN vigipirate.gouv.fr

Formation à la sécurité du numérique – MOOC | ANSSI secnuacademie.gouv.fr

Charte de bonnes pratiques en matières d'achats de prestations de sécurité privée | interieur.gouv.fr

Plan VIGIPIRATE : Faire face ensemble | sgdsn.gouv.fr

Référent sûreté | referentsurete.fr

SGDSN
SECRÉTARIAT GÉNÉRAL
DE LA DÉFENSE ET DE
LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
sgdsn.gouv.fr

Maquette : Pôle Graphisme, Déplacement, Fabrication, Images – DSAF/DPSG – Décembre 2021.