PRÉFET DES ALPES-MARITIMES

Liberté
Égalité
Fraternité

Cabinet
Direction des sécurités
Service interministériel de défense et de protection civiles

Nice, le **12 janvier 2024**

VIGIPIRATE
SECURITE RENFORCEE
RISQUE ATTENTAT

Le préfet des Alpes-Maritimes
à
Mesdames et messieurs les maires
Monsieur le président du conseil régional
Monsieur le président du conseil départemental
Mesdames et messieurs les présidents d'établissements
de coopération intercommunale

(pour instruction et information aux destinataires in fine)

Objet : Adaptation de la posture VIGIPIRATE **"hiver - printemps 2024"**.
Abaissement au niveau ""sécurité renforcée - risque attentat"

Réf. : Plan gouvernemental VIGIPIRATE du 1er décembre 2016 (édition mai 2019).

P. J. : Logo VIGIPIRATE "sécurité renforcée - risque attentat".

La posture Vigipirate **"hiver - printemps 2024"** est applicable à compter du 15 janvier 2024. Elle ramène l'ensemble du territoire national au niveau **"sécurité renforcée – risque attentat"** et prendra fin début mai, à l'arrivée de la flamme olympique sur le territoire national. La période des Jeux olympiques et paralympiques (JOP) de Paris 2024 fera en effet l'objet d'une posture Vigipirate particulière.

Cette posture Vigipirate adapte le dispositif en mettant l'accent sur :

- la sécurité des bâtiments à usage d'enseignement et des lieux de culte ;
- la sécurité des rassemblements festifs, culturels et religieux ;
- la sécurité des transports et des bâtiments publics et institutionnels.

1. Sécurisation des lieux de rassemblement culturels et festifs

1) Lieux de rassemblement

La capacité à faire face à une attaque terroriste dans les lieux de rassemblement de personnes demeure une priorité essentielle.

Le renforcement des échanges d'information entre les organisateurs et les services de l'État reste capital. Préalablement à l'organisation de tout événement, les responsables et initiateurs doivent impérativement prendre contact avec les forces de sécurité intérieure (FSI) et les services préfectoraux, quand bien même l'avis des référents sûreté départementaux de la police ou de la gendarmerie a été sollicité.

Les responsables de sites sont invités à adapter les mesures de sûreté qui leur incombent en fonction des vulnérabilités particulières des lieux, de la fréquentation et des amplitudes horaires d'ouverture (jour/nuit), du contexte local évalué avec les services de l'État. Les personnels de l'équipe d'organisation seront sensibilisés aux bons comportements à adopter en cas de situation suspecte, de menace d'attaque terroriste, de confinement ou d'évacuation selon les situations.

2) Lieux de culte

Lors des fêtes religieuses, la sécurité devra être renforcée autour des lieux de culte avec un effort sur la présence visible des forces de l'ordre.

Je vous demande, lors de ces événements, de mobiliser vos moyens de vidéoprotection ainsi que vos policiers municipaux lorsque vous en disposez. En liaison avec les autorités religieuses locales, la mise en oeuvre de mesures de contrôle des accès (limitation du nombre d'accès, contrôles visuels des flux entrants à la diligence des équipes communautaires ou paroissiales) est recommandée.

Une attention particulière devra être portée aux véhicules en stationnement à proximité des lieux de rassemblement ou du culte. A cet égard, vous pourrez, si nécessaire prendre des mesures temporaires d'interdiction de circuler et de stationner.

3) Mesures propres aux périodes de vacances scolaires

Les lieux sujets à de fortes affluences saisonnières durant les vacances scolaires (stations de sports d'hiver, salles de spectacles, etc.) bénéficieront de moyens adaptés. Les services de l'État (forces de sécurité intérieure et unités Sentinelle) adapteront leur dispositif en conséquence.

J'invite les opérateurs à solliciter l'appui des référents sûreté départementaux de la police ou de la gendarmerie nationales.

2. Sécurisation des grands espaces de commerce, de tourisme et de loisirs

Les lieux de commerce, les espaces de loisirs et les sites touristiques majeurs restent des cibles privilégiées.

1) Sites touristiques

Compte tenu de la situation internationale et de la persistance de la menace, les mesures de vigilance doivent être enforcées par les exploitants de ces sites.

Les lieux sujets à de fortes affluences saisonnières durant les vacances scolaires (stations balnéaires, salles de spectacles, etc) bénéficieront de moyens adaptés. Les services de l'État (forces de sécurité intérieure et unités Sentinelle) adapteront leur dispositif en conséquence.

Les polices municipales demeurent également mobilisées.

2) Espaces de commerce

La sécurité sera renforcée autour des grands espaces de rassemblements ayant pour objet des activités commerciales, notamment lors des soldes, marqués par une forte affluence.

En cas de vulnérabilité particulière signalée, les responsables de sûreté des établissements concernés devront adapter leur dispositif par la mise en oeuvre de mesures de protection et de contrôle spécifiques telles que :

- la sensibilisation des personnels aux comportements à adopter en cas de situation suspecte, de menace d'attaque terroriste, de confinement ou d'évacuation ; par ailleurs, les responsables d'enseignes sont incités à former leur personnel aux gestes de premiers secours.

- la mise en place ou l'adaptation de conventions locales de coopération de sécurité avec les forces de sécurité ;

- l'utilisation d'un dispositif de détection du passage à l'acte dans et aux abords des établissements (vidéoprotection, agents privés de sécurité).

Sur la voie publique, la vidéoprotection peut être mise en oeuvre par les personnes morales, sur autorisation préfectorale, pour la protection des abords immédiats de leurs bâtiments et installations dans les lieux susceptibles d'être exposés à des actes de terrorisme.

Dans la mesure du possible, je pourrais accorder l'extension de cette vidéosurveillance aux abords immédiats de la voie publique et aux espaces de commerce.

De même, je pourrais autoriser, à titre exceptionnel, la présence d'agents privés de sécurité, même itinérants, sur la voie publique, aux abords des sites des espaces de commerce qui en feront la demande.

3. Sécurisation des transports collectifs

Les transports présentent de nombreuses vulnérabilités face à la menace terroriste et restent une cible privilégiée notamment au moment des pics de fréquentation (*périodes de vacances, évènements sportifs ou festifs,..*). À ces occasions, le niveau de sécurité des plateformes aéroportuaires, des gares, des ports et des réseaux de transport en commun devra être renforcé.

1) Espaces d'accueil des voyageurs pour tout mode de transport

La menace visant les emprises des gares, des aérogares et des stations de tramway impose une vigilance quotidienne et redoublée sur les espaces d'accueil des voyageurs, notamment durant les périodes d'affluence.

2) Spécificité du transport aérien

Les gestionnaires d'aéroports et les compagnies aériennes maintiendront leur haut niveau de vigilance lors des contrôles d'embarquement des passagers.

Les services de l'État et la société anonyme "aéroports de la Côte d'Azur" mettront tout en œuvre pour garantir la sécurité de la zone accessible au public (zone côté ville).

Une coordination étroite entre les forces de sécurité intérieure, les armées, et les opérateurs, doit permettre une intervention rapide, et la communication envers des passagers ne maîtrisant pas la langue française doit être prise en compte.

3) Infrastructures et réseaux ferroviaires

Les transports terrestres constituent toujours une cible d'intérêt, à la symbolique et l'impact forts.

Toute information relative à une intrusion malveillante ou tentative de sabotage dans les infrastructures et les réseaux dédiés à la circulation des trains *(voies ferrées classiques, lignes grande vitesse, réseaux-interurbains,...)* doit faire l'objet d'une communication immédiate aux forces de sécurité intérieure locales.

Chaque incident doit être considéré avec la plus grande attention et faire l'objet d'un compte-rendu vers le centre ministériel de veille opérationnelle et d'alerte (CMVOA) du ministère de la transition écologique :

- téléphone : 01 40 81 76 20
- courriel : permanence.cmvoa@developpement-durable.gouv.fr

4) Transport maritimes de passagers

Il est demandé aux exploitants portuaires d'assurer la continuité du contrôle des véhicules, de leurs passagers et de leur chargement. Je vous rappelle que tout armateur exploitant des navires rouliers à passagers doit mettre en place un dispositif destiné à prévenir l'introduction des articles prohibés (armes à feu, explosifs...), par les personnes en sortie des espaces rouliers, au moment de leur accès aux espaces publics du navire.

4. Sécurisation des bâtiments publics et des établissements d'enseignement et de recherche, et des établissements de santé

Les installations et bâtiments publics tels que les sites institutionnels, dont les administrations, peuvent constituer des cibles potentielles ; c'est la raison pour laquelle vous devez prendre toutes les mesures nécessaires, en plus des mesures permanentes de vigilance, particulièrement aux abords des accueils du public.

Les établissements d'enseignement et de recherche sont, quant à eux, des cibles privilégiées, quelle que soit l'origine de la menace, en raison notamment de leur charge symbolique. L'attentat du 13 octobre 2023 à Arras confirme la sensibilité forte de ces établissements.

Je vous demande d'actualiser les annuaires de crise et les procédures d'alerte afférentes, ainsi que les plans de protection. Les procédures internes d'évacuation ou de confinement devront être portées à la connaissance des nouveaux arrivants.

Les attroupements seront réduits au minimum et les stationnements sauvages aux abords des établissements seront empêchés avec le concours des forces de sécurité.

Les vulnérabilités identifiées, sans qu'il ne s'agisse d'une liste exhaustive, requièrent un niveau élevé de sécurisation notamment par :

- le contrôle des flux de personnes, des marchandises et des véhicules ;
- le contrôle des sacs à l'entrée des établissements à chaque fois que cela est possible ;
- la surveillance active aux abords des établissements ;
- un contrôle des accès aux différents sites et emprises bâtimentaires ;
- le maintien du niveau de vigilance face aux messages d'alerte à la bombe avec levée de doute systématique.

Dans les établissements et les sites des opérateurs concernés, une attention particulière sera portée à la protection et aux contrôles des laboratoires sensibles soumis à une réglementation spécifique, ainsi qu'aux lieux de stockage de matières dangereuses (sources radioactives, produits toxiques ou agents pathogènes, précurseurs d'explosifs, matières biologiques, etc.) et lieux abritant des animaleries. Les zones considérées sensibles (zones à régime restrictif, zones sécurisées, zones d'accès restreint) doivent faire l'objet d'une vigilance maximale, de procédures de contrôle renforcées et de signalements systématiques.

S'agissant des établissements de santé, les actions mises en oeuvre par les forces de sécurité intérieure doivent être maintenus :

- la sécurisation des abords des établissements de santé de niveau 1 (selon la cartographie transmise par les agences régionales de santé) ;
- le renforcement immédiat, en cas d'attentat, des établissements accueillant des victimes, afin de prévenir les risques de sur-attentat.

Les directeurs d'établissement de santé s'assurent également de la mise en oeuvre des mesures de sûreté de leur plan de sécurisation d'établissement (PSE) d'autant plus à l'approche des jeux olympiques et paralympiques 2024.

5. Sécurisation du numérique

Les menaces visant les administrations et les entreprises privées restent élevées et variées (attaques par rançongiciels, attaques indirectes et vulnérabilités critiques entre autres).

Plusieurs entreprises, collectivités et établissements de notre département ont fait l'objet de cyber-attaques, avec des conséquences économiques, financières et réputationnelles importantes.

Afin de se tenir à jour du niveau de la menace et des mesures cyber préventives cyber prioritaires, il est préconisé de consulter régulièrement les sites suivants :

- https://www.cyber.gouv.fr (site de l'Agence nationale de la sécurité des systèmes d'information) ;

- https://www.cert.ssi.gouv.fr (site du centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques).

Objectifs de sécurité recherchés sur la période

Au regard de l'évaluation de la menace pour la sécurité du numérique présentée aux paragraphes supra, il apparait nécessaire d'appliquer les objectifs et mesures de sécurité suivants :

- **Déterminer l'ensemble des composants du système d'information (SI) contenant un logiciel/matériel particulier**

Le cycle de vie des équipements et applicatifs informatiques conduit à l'émergence de vulnérabilités susceptibles de conduire à la compromission des systèmes d'informations. Par ailleurs, certains éditeurs de solutions informatiques arrêtent la maintenance de technologies moins récentes, laissant ces technologies sans mise à jour disponible pour corriger d'éventuelles vulnérabilités.

Il est donc nécessaire de cartographier régulièrement son SI et les technologies le composant afin de pouvoir agir en cas de vulnérabilité et de fin de support d'une solution informatique. Cette cartographie doit permettre, à terme, d'identifier les composants du SI directement sous contrôle et ceux sous-traités. Ces travaux sont également susceptibles de supporter les travaux de construction de politiques de cybersécurité, de mettre en

place une approche basée sur les risques ou de traiter plus efficacement les incidents de sécurité.

L'ANSSI propose en ce sens un guide permettant de mettre en place un processus de cartographie des SI (https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation). Un exemple récent de ce phénomène est la fin du support de WINDOWS SERVER 2012 et 2012 R2. Ce système d'exploitation pour serveur répandu n'est plus supporté par l'éditeur Microsoft depuis le 10 octobre 2023. Il est donc nécessaire d'identifier la présence de ce système d'exploitation sur son système d'information et de lancer une projet de migration vers une version supportée, et d'isoler a minima les serveurs impossible à migrer à date.

- **Rechercher sur le SI des marqueurs particuliers correspondant à une attaque**

Compte tenu des campagnes d'exploitation des vulnérabilités sur les services numériques, il est recommandé de prendre connaissance des marqueurs de compromissions publiés par l'ANSSI via les rapports de la menace (https://www.cert.ssi.gouv.fr/cti/) ou au travers du feed MISP public mis à disposition par l'ANSSI (https://misp.cert.ssi.gouv.fr/feed-misp). Ces marqueurs peuvent être complétés par d'autres sources de marqueurs provenant de partenaires de confiance.

Dans la mesure du possible, il convient d'ajouter ces marqueurs aux systèmes de détection disponibles (antivirus, EDR, NIDS, HIDS, etc.). Par ailleurs, il est recommandé de chercher la présence de ces marqueurs sur l'historiques des journaux disponibles afin d'identifier d'éventuelles tentatives de compromission.

- **Consulter régulièrement les sources d'information relatives aux vulnérabilités et attaques (site Internet du CERT-FR)**

Afin de se prémunir d'éventuelles attaques suite à la découverte de vulnérabilités, il convient de mettre en place un processus de veille concernant la publication de vulnérabilités relatives aux éléments du SI.

Il est notamment possible de s'appuyer sur les bulletins du CERT-FR (https://www.cert.ssi.gouv.fr/avis/ et https://www.cert.ssi.gouv.fr/alerte/).

Cette veille sur les vulnérabilités doit être réalisée de manière quotidienne, idéalement via un processus automatisé à partir de sources complémentaires pour couvrir l'ensemble des briques du système d'information.

- **Absorber le trafic illégitime au niveau du réseau**

Compte tenu des attaques menées par DDoS (déni de service distribué), il est important de s'assurer que les opérateurs de services numériques, d'une part, disposent d'infrastructures et composants de sécurité permettant d'absorber le trafic et qu'ils puissent transmettre à leurs clients une liste d'adresses IP illégitimes à bloquer et d'autre part, qu'ils assurent le renforcement des leurs systèmes d'information et des sites web hébergés. L'ANSSI a récemment publié une fiche pratique sur la mise en place d'un service de protection anti-DDoS, disponible sur son site web (https://cyber.gouv.fr/publications/les-denis-de-service-distribues-ddos).

Sur la base des informations transmises par l'ANSSI, il est nécessaire d'identifier les moyens de filtrage les plus efficaces (par exemple avec un équipement en entrée de

réseau ou avec l'appui d'un opérateur de communication électronique ou un fournisseur de solution spécialisé). Il est recommandé de prendre en compte les différentes typologies d'attaques par déni de service (au niveau applicatif, spécifique à protocole ou basé sur la volumétrie) et la couverture offerte par les moyens de filtrage. Les organisations doivent ensuite mettre en place ces mécanismes de protection anti-déni de service sur les infrastructures qu'ils hébergent ou demander la mise en place auprès des prestataires d'hébergement ou de communication le cas échéant.

- **Sensibiliser les utilisateurs sur un risque de sécurité et un comportement à adopter**

Dans le contexte d'importance des menaces d'origine cyber, il convient de sensibiliser régulièrement les utilisateurs aux risques numériques et à l'application de la politique de sécurité des systèmes d'information, en particulier vis-à-vis de l'utilisation de supports amovibles, de navigation Internet ou d'échanges de courriels.

L'attention à la sensibilité de l'information et à sa protection est également à intégrer au sein de cette sensibilisation. La non-séparation des usages et matériaux personnels et professionnels, échanges professionnels dans des lieux publics, présence de matériaux protégés ou classifiés sur des systèmes inadéquats sont à proscrire.

En complément, les utilisateurs privilégiées doivent être particulièrement sensibilisés aux bonnes pratiques afin de réduire les risques cyber. Les différents guides de l'ANSSI émettent de nombreuses recommandations en ce sens, qu'elles portentsur l'administration sécurisée des systèmes d'information (https://cyber.gouv.fr/publications/recommandations-relativesladministration-securisee-des-systemes-dinformation), de systèmes reposant sur l'Active Directory (https://cyber.gouv.fr/publications/recommandations-pour-ladministration-securisee-des-sireposant-sur-ad) ou lors la mise en place de politique de mots de passe (https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe).

Dans le cadre de cette sensibilisation, il est possible de s'appuyer sur SecNumacadémie (https://secnumacademie.gouv.fr/), la formation en ligne de l'ANSSI, qui détaille les bonnes pratiques pour une utilisation sécurisée des outils numériques.

- **Valider et appliquer un correctif de sécurité**

Face aux vulnérabilités critiques et à l'état de la menace, il est impératif d'appliquer, dans les plus brefs délais, les correctifs de sécurité mentionnés dans les bulletins d'alerte de sécurité du CERT-FR. Les correctifs référencés dans les alertes doivent, si cela est nécessaire et pour des raisons d'urgence et de criticité, être appliqués en dehors des processus de maintien en condition de sécurité des systèmes d'information. De même, les correctifs mentionnés dans les avis de sécurité et qui correspondent à la veille sur plus d'une centaine de produits, doivent également être appliqués dans le cycle habituel de maintien en condition de sécurité des systèmes d'information. L'exploitation de certaines des vulnérabilités référencées permet l'accès à des comptes privilégiés pour l'attaquant et étend ses capacités de latéralisation sur les systèmes. La bonne application des correctifs de sécurité référencés doit être régulièrement contrôlée et validée. Les bulletins d'alerte de sécurité et les avis de sécurité sont disponibles sur le site https://ww.cert.ssi.gouv.fr.

Les correctifs de sécurité et alertes du CERT-FR mentionnés ci-dessous doivent impérativement être appliqués pour corriger des vulnérabilités récentes particulièrement critiques :

✗ Vulnérabilités sur les équipements de sécurité en bordure des réseaux (alertes CERTFR-2023-ALE-008, CERTFR-2023-ALE-004 et CERTFR-2022-ALE-013 du CERT-FR)

De nombreux équipements comme les pares-feux et les passerelles VPN sont régulièrement la cible des attaquants qui continuent de trouver des vulnérabilités leur permettant de les compromettre en prendre pied dans le SI ou d'obtenir des secrets d'authentification pour usurper l'identité des utilisateurs. Pour certains produits, les vulnérabilités remontent à 2018 et continuent d'être exploitées. Les utilisateurs doivent impérativement mettre à jour ou faire mettre à jour ces équipements et procéder au renouvellement régulier des secrets d'identification (procédure extrêmement lourde) ou basculer sur des solutions d'authentification à multiples facteurs.

✗ Vulnérabilités sur les systèmes industriels (CVE-2023-39979 (MOXA), CVE-2023-29130 (Siemens), CVE-2023-29411 et CVE-2023-29411 (CVE-2023-29412)

Certains équipements, comme des automates programmables, sont exposés sur Internet sans aucune mesure de sécurité. Ces équipements particulièrement vulnérables peuvent être manipulés à distance par des attaquants afin de compromettre les réseaux industriels. Les utilisateurs de ces systèmes doivent vérifier la nécessité de maintenir une accessibilité de ces équipements à distance et, si cela s'avère le cas, mettre en place les mesures permettant de limiter l'accès à ces équipements par les seules acteurs ayant besoin de s'y connecter (équipements de filtrage, réseau privé virtuel, lien réseau dédié).

- **Adapter les dispositifs de réponse à incidents aux caractéristiques de la menace**

Afin de s'assurer d'être en mesure de répondre de manière rapide et efficace à un incident de sécurité informatique, il est nécessaire de construire un dispositif de réponse adéquat. En particulier, l'identification des ressources humaines en mesure d'armer les centres opérationnels de réponse est nécessaire, en passant si besoin par la contractualisation de prestataires de réponse aux incidents de sécurité (PRIS) pour renforcer l'action des équipes internes.

En complément, la définition d'une procédure-cadre de gestion des incidents ainsi que de fiches réflexes pour les scénarios d'attaques les plus pertinents pour l'organisation (chiffrement d'unposte, DDoS, exfiltration de données, etc.) permettent de mettre en oeuvre rapidement la réponse à incident, et donc d'en réduire la portée de manière significative.

Enfin, les organisations doivent également vérifier qu'un plan de continuité d'activité (PCA), détaillant les besoins de continuité de leur centre opérationnel, existe et puisse être mobilisé pour assurer la continuité de la réponse en cas d'incident, même de nature non-cyber (disfonctionnement électrique, télécoms, indisponibilité bâtimentaire, etc.). Les moyens de continuité identifiés via le PCA doivent être vérifiés via des tests et des exercices afin d'assurer de leur parfaite disponibilité et efficacité en cas d'incident les mobilisant.

- **Réaliser des tests de restauration des sauvegardes**

Afin de s'assurer de la capacité d'une reprise rapide de l'activité en cas d'attaque destructive et d'entrainer les équipes en charge de ces opérations, il convient d'organiser régulièrement des tests de restauration des sauvegardes réalisées sur les systèmes d'information. Ces tests, qui doivent être effectués sur les sauvegardes en ligne et hors-ligne, sont une opportunité de vérifier la présence des sauvegardes, leur qualité et

l'aptitude à restaurer un système d'information à partir de ces dernières. Le guide « d'hygiène numérique » de l'ANSSI apporte des précisions vis-à-vis de la mise en place de politiques de sauvegarde et de réalisation des tests : https://cyber.gouv.fr/publications/guide-dhygiene-informatique.

6. Consignes particulières

1) Sensibilisation des personnes en tenue

Les représentants de l'autorité publique (policiers, gendarmes, douaniers, militaires, personnels pénitentiaires) portant un uniforme, ou une tenue avec des signes distinctifs, constituent des cibles privilégiées. Elles devront être sensibilisées et informées par leurs autorités de tutelle des mesures de sécurité à appliquer.

2) Sensibilisation à la menace des attaques par véhicules-béliers

Les attaques par véhicules-béliers demeurent un mode d'action privilégié des organisations terroristes. Les organisateurs d'événements de voie publique doivent prendre en compte cette menace et mettre en oeuvre des dispositifs adaptés afin de s'en prémunir. Ils peuvent pour cela solliciter l'avis des référents sûreté locaux et/ou consulter :

- la fiche de recommandations Vigipirate « Se protéger contre les attaques au véhiculebélier», disponible sur le site Internet du SGDSN : https://www.sgdsn.gouv.fr/vigipirate ;

- le guide du ministère de l'intérieur accessible via le lien suivant : https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenements-de-voie-publique.

3) Signalement des cas suspects de radicalisation, des troubles comportementaux ou psychiatriques/psychologiques

La radicalisation se caractérise par un changement de comportement qui peut conduire certaines personnes à l'extrémisme ou au terrorisme. Des troubles psychologiques peuvent offrir un terreau favorable à la radicalisation. L'objectif du signalement au centre national d'assistance et de prévention de la radicalisation (CNAPR) est de protéger ces personnes contre elles-mêmes et la population contre de possibles comportements violents. Les combinaisons de comportements suivants doivent éveiller la vigilance et méritent de faire l'objet d'un signalement : changements physiques, vestimentaires et alimentaires, propos asociaux, passage à une pratique religieuse hyper ritualisée, rejet de l'autorité, repli sur soi, rejet brutal des habitudes quotidiennes, refus du débat, rejet de la société et des institutions, modification soudaine des centres d'intérêt, discours complotiste ou apocalyptique, tentative d'imposition agressive d'un ordre religieux.

Le signalement des cas suspects de radicalisation, quel que soit le type de radicalisation (religieuse, politique, etc.) se réalise de la manière suivante :

- **Appel au numéro vert : 0 800 005 696**

En cas de suspicion d'une action violente ou de tout autre cas d'urgence, appeler immédiatement le 17 ou le 112 pour alerter les forces de sécurité intérieure.

Des actions de sensibilisation sont conduites au sein de la fonction publique (cf. guide de la prévention de la radicalisation de la fonction publique-DGAFP 2019/ lois et principes de la République). Il importe également de rappeler l'existence d'un référent radicalisation/sécurité en préfecture qui a vocation à servir d'interlocuteur local pour cette problématique.

Le récent attentat à Paris le 2 décembre (pont de Bir Hakeim) a mis en exergue le profil d'un individu déjà condamné pour terrorisme, sorti en 2020 de détention, et sujet parallèlement à des troubles du comportement. Les troubles du comportement font l'objet d'une attention toute particulière et de dispositifs d'évaluation et de prise en charge ad hoc portés, notamment, par les circulaires Intérieur - Santé des 26 avril 2021 et 28 octobre 2022, avec des rappels réguliers.

Chaque événement terroriste donne en outre lieu à des conseils de vigilance particuliers, adaptés à l'évolution de la menace, ainsi qu'à des consignes précises, notamment au sein des groupes d'évaluation départementaux de la radicalisation islamiste, sous la responsabilité du MIOM.

4) Vigilance et mesures de prévention face au risque NRBC-E (nucléaire, radiologique, biologique, chimique, explosif)

Les récents attentas ou actes de malveillance commis ou déjoués en Europe ont démontré une capacité à fabriquer des explosifs artisanaux ou des substances toxiques à partir de produits chimique d'usage courant.

La recrudescence d'envois de lettres ou de colis piégés a justifié l'envoi d'un bulletin *flash* le 13 décembre 2022. Au moindre doute sur le contenu d'un colis ou d'une enveloppe, ce dernier ne doit pas être manipulé. Il doit être contrôlé au moyen d'un détecteur à rayons X.

En cas de d'impossibilité à mettre en oeuvre ce type de technologie, il convient d'alerter les forces de sécurité intérieure (appel au 17 ou au 112) et d'établir un périmètre de sécurité en faisant évacuer et en balisant la zone.

7. Sensibilisation du grand public

Vous veillerez à la sensibilisation du public accueilli dans vos locaux par l'affichage du logogramme correspondant au niveau du plan VIGIPIRATE actuellement en vigueur sur le territoire national **"Sécurité renforcée - risque attentat"**. Il doit être apposé de façon visible à l'entrée, dans les halls d'accueil et les lieux de passage du public.

Ce logogramme peut être téléchargé sur le site du SGDSN à partir du lien suivant : https://www.sgdsn.gouv.fr/vigipirate/le-plan-vigipirate-faire-face-ensemble

La communication des mesures et des comportements à adopter en cas d'attaque terroriste au sein des établissements recevant du public doit être renforcée.

Elle peut se faire par le biais de l'affiche "Réagir en cas d'attaque terroriste" qui peut être téléchargée sur le site du gouvernement (https://www.gouvernement.fr/reagir-attaque-terroriste) et imprimée sur un format adapté au lieu, placée et visible du public.

En complément de ce dispositif, une affichette intitulée "**les gestes d'urgence si quelqu'un a été blessé autour de vous**" téléchargeable à partir du lien précité pourra être diffusée sur les réseaux sociaux.

Enfin, je vous rappelle que le SGDSN a développé une **plateforme de sensibilisation VIGIPIRATE**. Il s'agit d'un outil pédagogique accessible au plus grand nombre qui permet, en quelques heures, d'être sensibilisé à la menace terroriste et d'avoir une meilleure connaissance des gestes et réflexes à adopter afin de prévenir un acte terroriste ou de réagir en cas d'attaque : https://www.sgdsn.gouv.fr/vigipirate/le-plan-vigipirate-faire-face-ensemble

8. Sensibilisation des professionnels

Dans un souci de large diffusion des bonnes pratiques face à la menace terroriste, des fiches de sensibilisation sont accessibles en ligne depuis l'espace Vigipirate du site internet du SGDSN ((https://www.sgdsn.gouv.fr/vigipirate/les-affiches-de-sensibilisation). Elles traitent des sujets suivants :

- que faire en cas d'exposition à un gaz toxique ?
- réagir en cas d'attaque terroriste.

La communication des mesures et des comportements à adopter en cas d'attaque terroriste au sein des établissements et lieux recevant du public est fondamentale. Aussi, ces affiches peuvent être téléchargées et imprimées sur un format adapté au lieu où elles sont placées afin de les rendre visibles du public (privilégier les entrées et sorties des établissements, les halls et salles d'attente).

Par ailleurs, un ensemble de fiches de recommandations et de bonnes pratiques à l'attention du grand public est également téléchargeable sur le site du SGDSN (https://www.sgdsn.gouv.fr/vigipirate/les-fiches-de-recommandation-et-de-bonnes-pratiques) :

- recommandations à l'attention des gestionnaires de parc et loueurs de véhicules (prévention des attaques au véhicule bélier) ;
- signalement des situations suspectes ;
- sécurisation de son établissement lors des journées porte-ouvertes ;
- organisation d'un confinement face à une menace terroriste;
- signalement de tout vol ou utilisation suspecte de produits chimiques ;
- sécurité du numérique : l'hameçonnage (ou *phishing*) ;
- recommandations pour la sécurisation des lieux de rassemblements ouverts au public ;
- sécurité du numérique : sensibilisation des dirigeants ;
- se protéger contre les attaques au véhicule bélier ;

- préparer ses déplacements et voyages à l'étranger ;
- gui des bonnes pratiques pour la sûreté des espaces publics ;
- prévention et signalement des cas suspects de radicalisation ;
- règles d'utilisation des drones et mesures de prévention face à un usage malveillant ;
- chaîne d'alerte face à une menace.

En complément, plusieurs guides de bonnes pratiques, à destination des élus et des professionnels, sont également téléchargeables sur le site du SGDSN (https://www.sgdsn.gouv.fr/vigipirate/les-guides). La version publique du plan Vigipirate "*Faire face ensemble*", également disponible en langue anglaise, peut aussi y être téléchargée.

Enfin, deux modules de formation en ligne, développés en liaison avec de nombreux partenaires, sont accessibles (https://vigipirate.gouv.fr) :

- un module long, dédié essentiellement aux professionnels de la sécurité ;
- un module court, prochainement disponible en plusieurs langues, dédié au grand public.

Ces modules intègrent notamment des témoignages vidéo, de citoyens ou de professionnels, ayant été confrontés à des attaques ou à des prises d'otages, ou dont les services contribuent au quotidien à lutter contre le terrorisme. Ils permettent, en quelques heures, d'être sensibilisé à la menace terroriste et d'avoir une meilleure connaissance des gestes et réflexes à adopter afin de prévenir un acte terroriste ou de réagir en cas d'attaque.

Dans un contexte géopolitique de fortes tensions et de menaces protéiformes, je vous appelle à la plus grande vigilance et sais pouvoir compter sur votre vigilance et votre implication dans la mise en oeuvre de ces mesures.

Le Préfet des Alpes-Maritimes

Hugues MOUTOUH