



PRÉFET DU PAS-DE-CALAIS

*Liberté
Égalité
Fraternité*

Service Interministériel de Défense et Protection Civile
Pôle Sûreté-Défense
Affaire suivie par Isabelle Thothe
03 21 21 20 34
isabelle.thothe@pas-de-calais.gouv.fr

Direction des Sécurités

Arras, le 12 janvier 2024

Le préfet du Pas-de-Calais

à

Mesdames et Messieurs les Maires

Monsieur le Président de l'AMF 62

Mesdames et Messieurs les Présidents des EPCI

Monsieur le Président du Conseil Départemental

En communication à Mesdames et Messieurs les Sous-Préfets d'arrondissement

OBJET : VIGIPIRATE – Adaptation à la posture VIGIPIRATE « hiver - printemps 2024 ».

La posture du plan VIGIPIRATE «Hiver – printemps 2024» est applicable à compter du 15 janvier 2024. L'ensemble du territoire national est placé au niveau « *Sécurité renforcée – Risque attentat* ». Elle prendra fin début mai, à l'arrivée de la flamme olympique sur le territoire national. *La période des jeux olympiques et paralympiques de Paris 2024 fera l'objet d'une posture vigipirate particulière qui devrait être activée dès le 1^{er} mai.*

La posture « hiver – printemps 2024 » met l'accent sur la sécurité des bâtiments à usage d'enseignement, des lieux de culte et des bâtiments publics et institutionnels. Les mesures BAT 12-01 et BAT 12-03 sont maintenues et visent :

- à réglementer le stationnement et/ou la circulation aux abords des installations et bâtiments ;
- à surveiller et contrôler les abords des installations et bâtiments.

Une vigilance particulière devra également être portée en direction des rassemblements liés aux manifestations religieuses, sportives et culturelles propres à la période. Il est notamment recommandé de porter l'effort de surveillance et de contrôle sur les rassemblements liés à la préparation des jeux olympiques et paralympiques ainsi que ceux qui pourraient être organisés en plein air dans le cadre de l'olympiade culturelle.

L'effort de protection est renforcé par la mesure RSB 12-05 qui vise à mettre en œuvre des dispositifs de protection, notamment pour prévenir la menace associée aux attaques par véhicules béliers.

Enfin, des mesures spécifiques numériques sont maintenues ou activées face aux menaces d'origine cyber.

I – sécurité des jeux olympiques et paralympiques 2024, des tests events préalables et des grandes manifestations sportives

Des « tests events », des grandes manifestations sportives et événements promotionnels préalables aux JOP 2024 seront organisés pendant la période couverte. Ils devront faire l'objet d'un effort particulier de sécurisation en lien avec les organisateurs. Une vigilance particulière devra être apportée à la sécurité des délégations potentiellement sensibles.

II - Sécurité des lieux de rassemblement et des lieux de culte

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'informations 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 FSI et les services préfectoraux. Ils peuvent également solliciter l'avis des référents sûreté départementaux de la police ou de la gendarmerie.

Les responsables de site sont toujours invités à adapter les mesures de sûreté qui leur incombent en fonction des vulnérabilités des lieux, de la fréquentation et des amplitudes horaires d'ouverture, et du contexte local. La sensibilisation de l'équipe d'organisation aux bons comportements à adopter en cas de situation suspecte, de menace d'attaque terroriste, de confinement ou d'évacuation selon les situations, est essentielle.

Concernant les mesures propres aux fêtes religieuses, la sécurité sera renforcée autour des lieux de culte avec un effort sur la présence visible des forces de l'ordre selon un mode de sécurisation dynamique, assorti de prises de contact avec les responsables de lieux de culte, voire statique s'agissant de sites signalés comme sensibles voire très sensibles par les autorités religieuses.

En liaison avec les autorités religieuses locales, la mise en œuvre 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. De la même façon, une attention particulière devra être portée aux véhicules en stationnement à proximité des lieux de rassemblement ou de culte.

A cet égard, je vous invite à prendre, dès que nécessaire, des mesures temporaires d'interdiction de circulation et de stationnement.

Les militaires de l'opération Sentinelle pourront appuyer le dispositif des forces de l'ordre dans le cadre de la mesure BAT 13-04 qui prévoit la possibilité de faire appel aux armées pour des missions de protection des installations et bâtiments désignés et de la population se trouvant aux abords immédiats.

Lors des périodes de vacances scolaires, les lieux sujets à de fortes affluences saisonnières bénéficieront de moyens adaptés. Les services de l'État (Forces de Sécurité Intérieure et unités Sentinelle) adapteront leur dispositif en conséquence. Vous pouvez solliciter l'appui des référents sûreté départementaux de la police nationale ou de la gendarmerie nationale.

Je vous rappelle la disponibilité d'un Guide des bonnes pratiques de sécurisation d'un événement de voie publique, disponible sur le site internet <https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenements-de-voie-publique>

Il peut être utilement complété du guide des bonnes pratiques pour la sûreté des espaces publics accessible via le lien <https://www.sgdsn.gouv.fr/vigipirate/les-guides>.

III – Sécurité 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.

La sécurité restera renforcée autour des grands espaces de rassemblement, ayant pour objet des activités commerciales (salons d'expositions, foires, etc.). Les interconnexions de transports en milieu clos dotées de commerces (gares, etc.) demeurent des points de vigilance.

Les lieux de tourisme, les stations balnéaires et les parcs de loisirs, particulièrement fréquentés pendant la période des vacances scolaires, les grands espaces de commerce lors des soldes d'hiver, demeurent un axe d'attention majeur.

La sécurisation des grands espaces de commerce, des sites de tourisme et de loisirs, implique notamment :

a/ La sensibilisation des personnels assurée par les gestionnaires de centres et d'enseignes commerciales.

b/ Le renforcement des échanges et de la coordination entre acteurs publics et privés

Elle se matérialise par la mise en place ou l'adaptation de conventions locales de coopération de sécurité.

Je vous rappelle que la convention nationale du 19 février 2019 entre le secrétaire d'État auprès du ministre de l'Intérieur et les principales organisations professionnelles représentant les grandes surfaces commerciales, promeut des conventions locales « visant au développement d'un plan de sécurisation suivi et pérenne des espaces commerciaux ». Il est recommandé que ces établissements mettent en place un plan de sûreté et désignent un coordonnateur en gestion de crise.

Ces types de coopération animés dans le cadre de la police de sécurité du quotidien (PSQ) instaurent une confiance mutuelle et impulsent une dynamique d'échanges d'informations. Les espaces commerciaux seront encouragés à recourir à ce type de dispositifs.

c/ Un dispositif de détection de passage à l'acte dans et aux abords des établissements ou des sites disposant d'agents privés de sécurité ou d'un système de vidéoprotection

Les responsables de la sécurité du secteur marchand privilégient la surveillance dynamique des espaces, la détection des comportements suspects et le recours à la vidéoprotection.

J'examinerai, dans la mesure du possible, l'extension de la vidéosurveillance aux abords immédiats de la voie publique. Par ailleurs, pour les espaces complexes le justifiant, le recours à la notion de « périmètre vidéoprotégé » pourrait être envisagé.

De même, j'examinerai les demandes des espaces de commerciaux d'autoriser, à titre exceptionnel, la présence d'agents privés de sécurité, même itinérants, sur la voie publique, aux abords de leur site.

IV – Sécurité des transports collectifs

Les transports présentent de nombreuses vulnérabilités et restent une cible privilégiée notamment au moment des pics de fréquentation (périodes de vacances, événements sportifs ou festifs, etc.). À ces occasions, le niveau de sécurité des plateformes aéroportuaires, ferroviaires, des gares, des ports et des réseaux de transport en commun sera renforcé.

V – Sécurité des bâtiments publics

Un effort particulier devra être porté sur la protection des sites préfectoraux et/ou interministériels situés hors du siège de la préfecture.

Vous veillerez à l'actualisation des annuaires de crise et des procédures d'alertes et à informer les nouveaux arrivants des plans de protection et des procédures internes d'évacuation ou de confinement.

Une vigilance particulière sera également portée à la sécurité des palais de justice et des établissements pénitentiaires, notamment dans les contextes de « procès sensible » et renforcée lors des procès de personnes mises en cause pour faits de terrorisme. La sécurisation des juridictions dans ce contexte doit constituer un axe d'effort spécifique.

Je vous précise que cette vigilance peut également concerner :

- les structures de la protection judiciaire de la jeunesse (PJJ) qui prennent en charge des mineurs poursuivis pour association de malfaiteurs à but terroriste ;
- les services pénitentiaires d'insertion et de probation (SPIP) préparant l'insertion ou la réinsertion des personnes placées sous main de justice, dont certaines sont radicalisées et/ou condamnées pour terrorisme.

VI– Sécurité des établissements d'enseignement et de recherche, des structures d'accueil collectif de mineurs (ACM), des séjours de cohésion du SNU et des établissements publics relevant du ministère des sports et des jeux olympiques et paralympiques

L'adaptation de la mesure met l'accent sur :

- l'évaluation des mesures de sécurisation renforcée des établissements et activités relevant des Ministère de l'Education Nationale et de la Jeunesse (MENJ), Ministère de l'Enseignement Supérieur et de la Recherche (MESR), Ministère des Sports et des Jeux Olympiques et Paralympiques (MSJOP) avec le concours des autorités localement compétentes et des forces de sécurité intérieure ;

- le maintien du niveau de vigilance face aux messages d'alerte à la bombe avec levée de doute systématique en lien avec les autorités localement compétentes ;
- l'organisation ministérielle et les liens entre services de l'État et opérateurs dans le cadre des JOP 2024 ;
- le maintien d'une haute vigilance quant à la sécurisation des systèmes d'information au regard de l'évaluation de l'ANSSI et des consignes relayées par le fonctionnaire de sécurité des systèmes d'information des MENS, MESR et MSJOP.

a/ Mesures de sécurisation des personnes et des biens

Les établissements d'enseignement et de recherche sont des cibles privilégiées en raison notamment de leur charge symbolique. L'attentat du 13 octobre 2023 à Arras confirme la sensibilité forte de ces établissements. Par conséquent, les établissements et organismes des MENJ/MESR et du Ministère de l'Agriculture et de la Souveraineté Alimentaire (MASA) doivent maintenir leur effort de sécurisation des personnes et des biens pour les personnels et les usagers.

Une attention particulière est également portée aux publics des centres régionaux des œuvres universitaires et scolaires, des structures d'accueil collectif de mineurs, des séjours de cohésion dans le cadre du Service National Universel.

Le partage d'information et les procédures d'alerte sont à actualiser et à renforcer entre les relais des MENJ/MESR/MSJOP (cabinets de recteurs, fonctionnaires sécurité défense, responsables sécurité/sûreté..), les préfetures et les Forces de Sécurité Intérieure.

Une haute vigilance des impacts des grands événements sportifs sur le périmètre du MSJOP devra être assurée, en lien notamment avec l'organisation interministérielle de suivi des JOP et l'opérateur Paris 2024. De plus, il est important que des liens renforcés soient déployés entre les régions académiques, les établissements du MSJOP, les préfetures et les collectivités territoriales hôtes afin d'organiser le partage d'informations et de gestion d'incidents ou d'évènements graves.

b/ Maintien d'une vigilance particulière des sites sensibles

Dans les établissements et les sites des opérateurs sous tutelle des MENJ/MESR et du MASA, 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.

VII– Sécurisation des sites touristiques, culturels et des expositions à thème sensible

Un haut niveau de vigilance doit être maintenu pour les Etablissements Recevant du Public (ERP) ainsi que les écoles et conservatoires relevant du Ministère de la Culture.

A l'approche des jeux olympiques et paralympiques, une série d'évènements labellisés « Olympiade Culturelle » se déroulent sur le territoire et sont particulièrement exposés du fait de leur association au mouvement olympique.

Pour ce qui concerne les événements se déroulant sur la voie publique, les organisateurs sont invités à se référer au guide des bonnes pratiques de sécurisation d'un événement de voie publique disponible sur le site Internet : <https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenements-de-voie-publique>.

VIII – Sécurité des opérateurs relevant des ministères sociaux

Les opérateurs des ministères sociaux (santé, solidarités ou travail) demeurent des cibles vulnérables. En raison de la situation internationale et des récents attentats terroristes commis sur le territoire national, les opérateurs veilleront à poursuivre la mise en œuvre des mesures vigipirate en lien avec les acteurs (Préfecture, FSI...).

a/ Secteurs santé et solidarité

Les préfetures veillent au maintien des actions mises en œuvre par les forces de sécurité intérieure concernant la sécurisation des abords des établissements de santé de niveau 1 (selon la cartographie transmise par les ARS) et le renforcement immédiat, en cas d'attentat, des établissements accueillant des victimes, afin de prévenir les risques de sur-attentat.

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

Je tiens à souligner les points d'attentions suivants :

- les opérateurs d'importance vitale devront être vigilants sur la mise à jour des documents de planification dans la perspective des JOP24 (dans la continuité de la crise sanitaire actuelle) ;
- les établissements de santé accueillant des mineurs dans le cadre du bilan somatique et médico-psychologique (conformément aux termes de l'instruction du 23 février 2018 relative à la prise en charge des mineurs de retour de zone d'opérations de groupements terroristes, notamment la zone irako-syrienne) ;
- les systèmes d'information qui sont des cibles régulières d'attaques du fait de leurs vulnérabilités. Le risque de cyberattaque est actuellement majoré.

b/ Secteur travail

Les agences et opérateurs chargés de la mise en œuvre locale des politiques de l'emploi peuvent constituer des cibles symboliques pour des individus souhaitant attaquer l'État.

IX– Protection des ressortissants et intérêts français à l'étranger (IFE)

Les actions et mesures de protection des ressortissants français, résidents ou de passage à l'étranger suivent trois axes :

a/ l'information et la sensibilisation

- édition des « Conseils aux voyageurs », régulièrement mis à jour ;
- recommandations sur les déplacements dans les zones « déconseillées sauf raison impérative » et « formellement déconseillées » et, au besoin, incitation à renoncer au déplacement ;
- conseil aux entreprises, opérateurs et ONG dans ces zones ;
- envoi de message d'alerte en temps réel en cas de risque d'enlèvement ou d'attentat ;
- incitation à l'inscription sur la liste Ariane des voyageurs ;
- réponse téléphonique active (24/7).

b/ la formation des agents des postes diplomatiques et consulaires à la gestion de crise et aux accidents collectifs.

c/ l'assistance aux victimes françaises en cas d'attaque terroriste à l'étranger :

- mise en œuvre d'une cellule de crise dans les ambassades ou à Paris ;
- élaboration de plans d'urgence destinés à organiser la prise en charge des victimes françaises ;
- suivi des familles des victimes d'actes terroristes et de prises d'otages à l'étranger.

Les actions de protection des implantations françaises à l'étranger et des agents de l'État portent sur les mesures de sécurité actives et passives ainsi qu'organisationnelles. Elles incluent des volets de formation renforcée, notamment des exercices de confinement/évacuation, de formation « comment réagir en cas d'attaque armée » et de formations longues « départ en postes sensibles ».

X – Sécurité du numérique

Les menaces visant les administrations et les entreprises privées restent élevées et variées (attaques par rançongiciels, attaques indirectes et vulnérabilités critiques). Afin de se tenir à jour du niveau de la menace et des mesures cyber préventives cyber prioritaires, il est recommandé de consulter régulièrement les sites suivants :

- <https://www.ssi.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).

De même, il convient d'appliquer les objectifs et mesures de sécurité suivants :

– **Mesure NUM 11-01** : déterminer l'ensemble des composants du SI contenant un logiciel/matériel particulier : il est en effet nécessaire de cartographier régulièrement son SI et les technologies le composant afin de pouvoir agir en cas de vulnérabilité. L'ANSSI propose un guide permettant de mettre en place un processus de cartographie des SI : <https://cyber.gouv.fr/publications/cartographie-du-systeme-d-information>).

- **Mesure NUM 11-02** : rechercher sur le SI des marqueurs particuliers correspondants à une attaque : à ce titre, 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 feedMISP public mis à disposition par l'ANSSI (<https://misp.cert.ssi.gouv.fr/feed-misp>).

– **Mesure NUM 21-02** : consulter régulièrement les sources d'information relatives aux vulnérabilités et attaques (site Internet du CERT-RF) :

il est recommandé de mettre en place un système de veille concernant la publication des vulnérabilités SI. Vous pouvez vous appuyer sur les bulletins du CERT-FR <https://www.cert.ssi.gouv.fr/avis> et <https://www.cert.ssi.gouv.fr/alerte>.

– **Mesure NUM 31-03** : absorber le trafic illégitime au niveau du réseau :

il est important de s'assurer que les opérateurs de services numériques disposent d'infrastructures et de composants de sécurité. L'ANSSI a récemment publié une fiche pratique sur la mise en place d'un service de protection, disponible sur son site web

<https://cyber.gouv.fr/publications/les-denis-de-service-distribues-ddos>

– **Mesure NUM 31-06** : sensibiliser les utilisateurs sur un risque de sécurité et un comportement à adopter :

il convient de sensibiliser régulièrement les utilisateurs aux risques numériques et à l'application d'une politique de sécurité des systèmes d'information, en particulier vis-à-vis des supports amovibles, de navigation internet ou d'échanges de courriels. Les personnels doivent également être sensibilisés à la sensibilité de l'information et à sa protection. Sont à proscrire la non-séparation des usages et matériaux personnels et professionnels, les échanges professionnels dans des lieux publics la présence d'informations protégés ou classifiés dans des lieux non protégés et inadéquats.

Une formation en ligne de l'ANSSI détaille les bonnes pratiques pour une utilisation sécurisée des outils numériques sur SecNumacadémie <https://secnumacademie.gouv.fr>.

– **Mesure NUM 41.01** : valider et appliquer un correctif de sécurité. Des correctifs de sécurité et alertes du CERT-FR ci-dessous doivent impérativement être appliqués pour corriger des vulnérabilités récentes particulièrement critiques :

- vulnérabilités sur les équipements de sécurité en bordure des réseaux : les utilisateurs doivent impérativement mettre à jour ou faire mettre à jour les équipements (ex : pare-feux, passerelles VPN) et procéder au renouvellement régulier des secrets d'identification ou basculer sur des solutions d'identification à multiples facteurs.

- vulnérabilités sur les systèmes industriels : les utilisateurs doivent vérifier la nécessité de maintenir une accessibilité de ces équipements à distance. En cas de nécessité, il convient de mettre en place des mesures permettant de limiter l'accès aux seuls utilisateurs ayant besoin de s'y connecter.

– **Mesure NUM 51-02:52-02** : adapter les dispositifs de réponse à incidents aux caractéristiques de la menace

Ceci implique la définition d'une procédure-cadre de gestion des incidents ainsi que des fiches réflexes pour les scénarios d'attaque les plus pertinents, l'existence d'un Plan de Continuité d'Activité, mobilisable en cas d'incident, y compris non cyber et la mise en place de vérifications (tests/exercices).

– **Mesure NUM 51-05** : réaliser des tests de restauration des sauvegardes.

Ces tests ont pour objectif de vérifier la qualité des sauvegardes et l'aptitude à restaurer un système d'information à partir de celles-ci. 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>.

XI – Consignes particulières de vigilance

Des consignes particulières de vigilance, de prévention et de protection sont à mettre en œuvre en matière de :

– **Sensibilisation des personnels en tenue** : toutes les personnes, civiles ou militaires, portant un uniforme ou une tenue avec des signes distinctifs, et représentant une autorité, constituent des cibles privilégiées. Il convient de les sensibiliser et de les informer des mesures de sécurité à appliquer.

– **Sensibilisation à la menace des attaques par véhicules-béliers** : les attaques par véhicules-béliers demeurent un mode d'action fréquemment utilisé par les organisations terroristes. Les organisateurs d'événements de voie publique doivent prendre en compte cette menace et mettre en œuvre les dispositifs adaptés afin de s'en prémunir. Ils peuvent solliciter l'avis des référents sûreté locaux et/ou consulter la fiche de recommandation « se protéger contre les attaques au véhicule-bélier », disponible sur le site <http://www.sgdsn.gouv.fr/vigipirate> ainsi que le guide du ministère de l'Intérieur <https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenements-de-voie-publique>

– **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 également 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 comportement suivantes doivent éveiller la vigilance et méritent de faire l'objet d'un signalement : changements physiques, vestimentaires et alimentaires, propos associatifs, 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...) se réalise en composant le numéro vert : **0 800 005 696**.

En cas de suspicion d'une action violente ou de tout autre cas d'urgence, vos services seront alertés via le 17 ou le 112.

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).

– *Vigilance et mesures de prévention face au risque NRBC-E.*

On constate une recrudescence d'envois de lettres ou de colis piégés. Au moindre doute sur le contenu d'un colis ou d'une enveloppe, l'objet ne doit pas être manipulé. Il doit être contrôlé au moyen d'un détecteur rayon X. En cas d'impossibilité, la consigne est d'alerter les Forces de Sécurité Intérieure et d'établir un périmètre de sécurité

Les professionnels vendant des explosifs artisanaux ou des substances NRBC ont l'obligation de signaler tout vol, disparition ou transaction suspecte au plateau d'investigation explosif et armes à feu (PIXAF) de la gendarmerie nationale, point de contact national pixaf@gendarmerie.interieur.gouv.fr ou 01 78 47 34 29 (24/7).

Pour rappel, la découverte de plis, colis ou contenants et substances suspectés de renfermer des agents NRBC dangereux relève de la gestion d'un trouble à l'ordre public quel que soit le traitement de cette découverte (administratif, judiciaire, sanitaire...).

– *Sensibilisation à la lutte anti-drone* : l'utilisation des drones est un mode d'action régulièrement mis en œuvre pour capter ou diffuser des images mais ceci peut évoluer vers des actes de malveillance ou terroristes. Les organisateurs doivent prendre en compte cette menace et solliciter l'avis des référents sûreté de la police ou de la gendarmerie nationales.

XII – Sensibilisation du grand public

Le niveau élevé de la menace exige le maintien d'une vigilance accrue. Les efforts de communication sont reconduits.

Vous veillerez notamment à l'utilisation du logogramme actuel « Sécurité renforcée – risque attentat ». Il peut être téléchargé sur le site du SGDSN : <https://www.sgdsn.gouv.fr/vigipirate/le-plan-vigipirate-faire-face-ensemble>. L'ensemble des guides de bonnes pratiques, à destination des élus et des professionnels, est également mis à disposition sur le site <https://www.sgdsn.gouv.fr/vigipirate/les-guides>.

De même, il convient de mettre en place des actions de sensibilisation envers les professionnels et le grand public. Dans un souci de pédagogie et de large diffusion des bonnes pratiques face à la menace terroriste, des fiches de sensibilisation, à destination du grand public ou de certains professionnels, sont accessibles sur le site internet du SGDSN : <https://www.sgdsn.gouv.fr/vigipirate/les-affiches-de-sensibilisation>.

La communication des comportements à adopter en cas d'attaque terroriste est également fondamentale. Des fiches sont également téléchargeables sur le site :

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

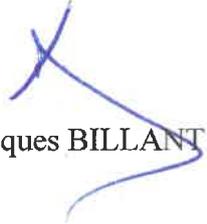
Enfin, deux modules de formation en ligne sont accessibles sur <https://vigipirate.gouv.fr> :

- 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 des témoignages vidéo de citoyens ou de professionnels. Ils permettent en quelques heures, d'être sensibilisé à la menace terroriste et d'avoir une meilleure connaissance des gestes et réflexes à adopter en vue, d'une part, de prévenir un acte terroriste et, d'autre part, de réagir en cas d'attaque.

Mes services se tiennent à votre entière disposition pour vous communiquer toutes les informations complémentaires que vous jugerez utiles.

Le Préfet,



Jacques BILLANT