PREMIER MINISTRE

Liberté
Égalité
Fraternité

Direction de la protection et de la sécurité de l'Etat

Secrétariat général de la défense et de la sécurité nationale

Paris, le

N° /SGDSN/PSE/PSN

Le secrétaire général de la défense et de la sécurité nationale

à

destinataires *in fine*

Objet : Adaptation de la posture VIGIPIRATE « été – automne 2021 ».

Références :
1. Plan gouvernemental Vigipirate n°10200/SGDSN/PSE/PSN/CD du 1er décembre 2016 (édition mai 2019).
2. Catalogue des fiches mesures Vigipirate (édition mai 2019).

Annexes :
1. Cartographie des attentats aboutis et déjoués en Europe de 2020 au 1er semestre 2021.
2. Historique des attentats en France de 2015 à juin 2021.
3. Cartographie coopération navale volontaire
4. Fiche pratique : drone.
5. Fiche pratique : signalement de radicalisation.

Pièce jointe : Tableau actualisé des mesures Vigipirate.

La nouvelle posture Vigipirate « *été – automne 2021* » sera active à compter du 19 juin 2021 et maintiendra l'ensemble du territoire national au niveau « ***sécurité renforcée - risque attentat*** ».

Dans le contexte de crise sanitaire générée par la pandémie de la COVID-19, la menace terroriste demeure à un niveau très élevé, comme l'illustrent la série d'attaques survenue en 2020 et au début de l'année 2021. Cette posture Vigipirate adapte donc le dispositif en mettant l'accent sur :

- la sécurité des bureaux de vote pour les élections régionales et départementales ;
- la sécurité des sites touristiques et des transports publics de personnes, en particulier lors des vacances scolaires et universitaires, en fonction de la reprise d'activité ;
- la sécurité des espaces de commerce et des lieux de rassemblement, y compris les lieux de culte ;
- la sécurité des bâtiments publics (services publics, locaux associatifs ou politiques, écoles et universités), avec une attention particulière sur les établissements de santé, médico-sociaux et sociaux, ainsi que la sécurité des sites de production, de stockage et de distribution des produits de santé, ainsi que des lieux de vaccination.

Après une description du contexte général et une évaluation de la menace, cette note de posture expose les différents objectifs de sécurité mais sans viser à être exhaustif. Chaque ministère en assurera sa déclinaison en prenant en compte sa vulnérabilité propre. Une version actualisée du tableau des mesures Vigipirate est jointe à la présente note.

En cas d'attaque ou d'évolution significative de la menace terroriste, cette posture Vigipirate est susceptible de faire l'objet d'une adaptation, en urgence, en liaison avec l'ensemble des ministères.

SOMMAIRE

1. [NP] Contexte général 4

1.1 Principaux événements sur le territoire national 4
1.2 Prolongation des contrôles aux frontières intérieures 4
1.3 Evolution du contexte juridique : texte adoptés fin 2020 – début 2021 4

2 [CD] Evaluation de la menace terroriste 7
[NP] Synthèse

3 [NP] Evaluation des principaux risques cyber sur la période couverte 7

3.1 Impacts constants de la crise sanitaire et des périodes de congés 7
3.2 Tendances actuelles des attaques et des vulnérabilités critiques 8
3.2.1 Attaques par rançongiciel 8
3.2.2 Attaques indirectes 8
3.2.3 Vulnérabilités critiques exploitées massivement par les cyberattaquants 8

4 [NP] Adaptation de la posture Vigipirate « été – automne 2021 » 9

5 Consignes particulières de vigilance, prévention et protection 17

6 Sensibilisation du grand public 17

Avertissement : ce document pris dans son ensemble est classifié *confidentiel défense*. Les paragraphes commençant par [CD] sont classifiés, ceux commençant par [DR] sont protégés. L'ensemble des autres paragraphes, [NP] ou non marqués , est diffusable sans restriction.

1. [NP] Contexte général

1.1 Principaux événements sur le territoire national

La période couverte par la posture « *été – automne 2021* » est marquée par :

- les élections régionales et départementales, au printemps 2021 ;
- les flux importants de voyageurs dans les transports collectifs de personnes lors des vacances estivales ;
- les modalités de gestion de la crise du COVID 19.

Le contexte particulier de la crise COVID rend impossible un récapitulatif des principaux événements (culturels, sportifs, religieux, commémoratifs, etc.). **Les mesures de sécurité sanitaires pour limiter la diffusion du virus, devront être évaluées par les autorités préfectorales** qui restent juges du niveau à atteindre pour encadrer la sûreté des manifestations à forte affluence ou au caractère symbolique marqué. La gestion des flux et des files d'attente devront ainsi faire l'objet d'une vigilance accrue.

1.2 Prolongation des contrôles aux frontières intérieures

La France a rétabli les contrôles aux frontières intérieures le 13 novembre 2015. Initialement prévu pour la durée de l'organisation de la COP 21 (Conférence des Nations-Unies pour le climat), c'est-à-dire du 13 novembre au 13 décembre 2015, le rétablissement de ces contrôles a, depuis, été régulièrement reconduit sur le fondement de l'article 25 du code frontières.

La France a informé la commission européenne de la reconduction du rétablissement des contrôles aux frontières intérieures jusqu'au 31 octobre 2021 du fait du niveau de menace mais aussi du contexte sanitaire. Si cette mesure ne devait pas être renouvelée, une information *ad hoc* serait transmise et les adaptations intégrées dans la posture.

1.3 Evolution du contexte juridique : texte adoptés fin 2020 – début 2021

- **Loi du 24 décembre 2020 relative à la prorogation des chapitres VI à X du titre II du livre II et de l'article L. 851-3 du code de la sécurité intérieure (JORF du 26 décembre 2020)**

Le texte prolonge jusqu'au 31 juillet 2021 différentes mesures de lutte contre le terrorisme dont le Parlement avait autorisé la mise en œuvre jusqu'au 31 décembre 2020 (fermeture administrative des lieux de culte, mesures de surveillance, technique de renseignement dite "algorithme"...).
Pour en savoir plus :
La loi prolonge la durée d'application des **mesures temporaires** instaurées par la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme **dite SILT** concernant :

- les périmètres de protection ;
- la fermeture administrative des lieux de culte pour apologie ou provocation au terrorisme ;
- les mesures individuelles de contrôle administratif et de surveillance notamment pour les sortants de prison condamnés pour des faits de terrorisme ou de détenus radicalisés ;
- les visites domiciliaires et saisies ;
- le contrôle parlementaire.

Ces mesures figurent aux chapitres VI à X du titre II du livre II du code de la sécurité intérieure. Elles ont accru les pouvoirs des services antiterroristes à la sortie de l'état d'urgence le 1er novembre 2017 .

Le texte prolonge par ailleurs d'un an, **jusqu'au 31 décembre 2021**, la **technique de renseignement dite "algorithme"** prévu par l'article L. 851-3 du code de la sécurité intérieure. Cette technique a été mise en place **à titre expérimental** par la loi du 24 juillet 2015 relative au renseignement, afin de détecter de façon précoce les menaces terroristes.

Est également reportée du 30 juin 2020 au 30 juin 2021 la date à laquelle le gouvernement doit remettre au Parlement un rapport sur l'application de cet article.

- **Loi pour une sécurité globale préservant les libertés (JORF du 26 mai 2021)**

Le texte contient diverses mesures relatives à la lutte contre le terrorisme. La loi porte sur les polices municipales, les sociétés de sécurité privées, les outils de surveillance et la protection des forces de l'ordre. Elle a été en partie censurée par le Conseil constitutionnel.

Elle élargit notamment aux actes de terrorisme les missions, même itinérantes, de surveillance que les agents privés de sécurité sont autorisés, par le préfet de département ou, à Paris, par le préfet de police, à exercer sur la voie publique contre les vols, dégradations et effractions visant les biens dont ils ont la garde (art. L.613-1 du CSI) .

- **Projet de loi relatif à la prévention d'actes de terrorisme et au renseignement**

Déposé fin avril à l'Assemblée nationale, ce texte, qui est actuellement en cours d'examen par le Parlement, doit permettre d'affiner les outils de lutte contre le terrorisme. En particulier il vise à **pérenniser certaines mesures inspirées de l'état d'urgence** : fermeture de lieux de culte, instauration de périmètres de protection, mesures individuelles de contrôle et de surveillance (comme le pointage) et les « visites et saisies ». Ces mesures inscrites dans la loi dite SILT d'octobre 2017 ont été reconduites jusqu'au 31 juillet 2021 par la loi du 24 décembre 2020.

Il prévoit également de renforcer la base légale du brouillage des drones malveillants effectué par les services de l'État concourant à la sécurité intérieure et à la défense nationale et le service public de la justice.

- **Ordonnance n° 2020-1544 du 9 décembre 2020 renforçant le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme applicable aux actifs numériques**

Le démantèlement, en France, au mois de septembre dernier, d'un réseau de financement terroriste recourant à des transactions en actifs numériques, rappelle l'existence de détournements criminels contre lesquels il est nécessaire de lutter. Afin de lutter plus efficacement contre ces risques de détournement et de protéger l'intégrité financière de l'économie française, cette ordonnance, prise sur le fondement de l'article 203 de la loi PACTE, soumet aux obligations posées par le code monétaire et financier les activités d'échanges d'actifs numériques contre d'autres actifs numériques (échanges dits « crypto-to-crypto ») et les plateformes de négociation d'actifs numériques. Elle complète ainsi le cadre juridique issu de la loi PACTE du 22 mai 2019 relative à la croissance et la transformation des entreprises. Cette ordonnance renforce en outre la lutte contre l'anonymat des transactions en actifs numériques en incluant les prestataires de services sur actifs numériques (PSAN) parmi les entités ayant l'interdiction de tenir des comptes anonymes.

- **Décret n° 2020-1452 du 27 novembre 2020 portant diverses dispositions relatives notamment à la procédure civile et à la procédure d'indemnisation des victimes d'actes de terrorisme et d'autres infractions**

Ce texte renforce les droits et garanties des victimes d'acte de terrorisme lors de l'examen médical réalisé à la demande du Fonds de garantie des victimes des actes de terrorisme et d'autres infractions (FGTI).

- **Décret n° 2021-446 du 15 avril 2021 renforçant le cadre de lutte contre le blanchiment de capitaux et le financement du terrorisme**

Le décret tire les conséquences au niveau réglementaire des modifications réalisées par l'ordonnance n° 2020-1544 du 9 décembre 2020 renforçant le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme applicable aux actifs numériques. L'article 1er limite le contrôle préalable en matière de lutte contre le blanchiment et le financement du terrorisme (LCB-FT) à l'exercice de l'activité aux deux premiers services sur actifs numériques (service de conservation pour compte de tiers, service d'achat et de vente d'actifs numériques contre de la monnaie ayant cours légal). L'article 2 complète la composition du Conseil d'orientation de la lutte contre le blanchiment des capitaux et le financement du terrorisme. L'article 3 étend ces dispositions à l'outre-mer.

2 [CD] Evaluation de la menace terroriste

[NP] Synthèse

Sept attaques terroristes abouties sur le territoire national en 2020 et 2021 ont causé **huit morts et onze blessés**. La menace terroriste, **d'origine essentiellement endogène**, se maintient à un niveau élevé, malgré l'affaiblissement des organisations terroristes extérieures et la dégradation importante de leurs capacités à projeter des attaques.

Plusieurs tendances se dégagent des dernières attaques réalisées sur le territoire national :

- Une **cristallisation** des divers courants islamistes sur la **question du blasphème** : dans le contexte de tensions initiées par la **republication, en septembre 2020**, des caricatures de Mahomet par *Charlie Hebdo* au début du procès des attentats de janvier 2015, les **quatre dernières attaques** réalisées en France, entre le 25 septembre 2020 et le 23 avril 2021, ont impliqué des individus dont le **passage à l'acte est lié**, de façon plus moins affirmée, **à ce sujet** ;
- Les prémices d'un **phénomène d'autonomisation de la menace** : commises par **des individus inconnus** des services de renseignement, **sans affiliation précise à un groupe terroriste,** les attaques recensées en France depuis 2019 **n'ont pas été revendiquées** par des organisations terroristes, ce qui révèle une **autonomisation opérationnelle et idéologique** des acteurs de la menace. La radicalisation des candidats à l'action violente est par ailleurs régulièrement facilitée par des **déséquilibres psychologiques**, voire des **pathologies mentales**.

Par ailleurs, depuis plusieurs années, le **niveau de la menace terroriste en prison est préoccupant**, bien qu'aucun projet terroriste lié à l'univers carcéral n'ait été enregistré récemment. Cette menace tient à la présence **d'un niveau élevé de détenus incarcérés pour terrorisme islamiste** auquel s'ajoute un **nombre conséquent de détenus de droit commun radicalisés**. La menace des terroristes **libérés de prison** constitue également un enjeu.

Parallèlement, **les origines de la menace terroriste se diversifient** en raison de la **polarisation croissante des idéologies** et de l'augmentation **des radicalités politiques**. Le risque d'action isolée **d'un sympathisant de l'ultra-droite**, de même que des actions concertées, émanant de groupes **complotistes et/ou conspirationnistes**, sont ainsi à redouter. A l'autre bout du spectre, si la mouvance **d'ultra-gauche** demeure principalement une menace de **voie publique**, le risque terroriste se confirme néanmoins, notamment via des **individus *de retour*** des théâtres de guerre ou **en provenance d'Italie ou de Grèce**, qui concentrent les mouvances anarchistes les plus radicales.

Si une attaque peut être conduite en tout lieu du territoire, **plusieurs cibles apparaissent prioritaires** parmi lesquelles : les **représentants en uniforme** de l'autorité publique tout comme **les lieux où ils résident**; les **grands rassemblements festifs** ; les **sites symboliques** ; les **lieux publics très fréquentés** ; **les établissements situés au cœur du fonctionnement de notre société** (écoles, universités, hôpitaux ...). En outre, la **fin d'année 2021 verra se tenir le procès des attentats du 13 novembre 2015,** qui va nécessiter une **logistique sécuritaire conséquente**, eu égard au nombre de parties concernées qui sont **autant de cibles potentielles** réunies sur un même site pendant plusieurs semaines.

La menace terroriste contre les **ressortissants et les intérêts français à l'étranger apparaît également élevée**, notamment dans la région du Sahel et contre des cibles symboliques (ambassades, lycées et écoles françaises ...).

De façon générale, les modes opératoires rudimentaires (utilisation d'armes par destination) demeurent privilégiés (armes blanches ou autres moyens sommaires, véhicule bélier, armes à feu). Toutefois, les modes **opératoires plus sophistiqués** (engins explosifs improvisés à base de TATP ou de matières inflammables), alimentés par l'accès à des tutoriels sur internet, ne doivent pas être négligés. De même, la **menace liée à l'utilisation de substances chimiques ou d'agents biologiques** est toujours à prendre au sérieux/ notamment en raison de l'intérêt qu'elle avait suscité auprès de l'El.

3 [NP] Evaluation des principaux risques cyber sur la période couverte

3.1 Impacts constants de la crise sanitaire et des périodes de congés

Les conséquences de la pandémie de la COVID-19 continuent d'influer fortement les habitudes de travail en imposant un recours intensif au télétravail et à l'utilisation quotidienne d'outils numériques.

Si les entreprises et administrations s'adaptent à ces nouvelles pratiques, le niveau de sécurité associé aux outils numériques et à leurs usages reste largement perfectible. Le manque de cloisonnement entre les systèmes d'informations professionnels et les outils personnels, peu ou pas sécurisés, facilite par exemple l'exécution d'attaques par hameçonnage (courriels avec lien ou pièce jointe malveillante) menées à des fins de captation de données ou de chantage par rançongiciel.

Par ailleurs, le rythme des présences et absences des employés lié à la situation est propice aux attaques informatiques puisqu'il permet aux attaquants d'exploiter la baisse de vigilance des utilisateurs. De plus, les missions de détection et de réponse aux incidents de sécurité ou de mise à jour des logiciels et des systèmes d'information peuvent être complexifiées par des effectifs restreints voire par l'absence des équipes de sécurité informatique.

3.2 Tendances actuelles des attaques et des vulnérabilités critiques

3.2.1 Attaques par rançongiciel

L'augmentation du nombre d'attaques par rançongiciel (données chiffrées via un logiciel malveillant, impliquant le paiement d'une rançon pour les déchiffrer) se poursuit depuis 2020 de façon significative (192 incidents rapportées à l'ANSSI en 2020 contre 54 en 2019).

Ces attaques touchent aujourd'hui tous les secteurs (éducation, santé, énergie, technologies, BTP) et toutes les organisations (entreprises privées - PME, CAC40 - et publiques - collectivités publiques, établissements de santé, universités). En France, sur ces derniers mois, elles ont particulièrement touché les secteurs de la santé (dont les hôpitaux) et des transports maritimes, en désorganisant leur fonctionnement habituel (ralentissement ou arrêt de certains services). Aux Etats-Unis, elles ont impacté le secteur de l'énergie en forçant la mise à l'arrêt d'un oléoduc pendant plusieurs jours.

Globalement, un rançongiciel peut affecter l'activité d'une entité sur plusieurs semaines voire plusieurs mois, l'obligeant à dépenser jusqu'à plusieurs millions d'euros pour sécuriser et relancer ses systèmes.

La montée en compétences techniques, la professionnalisation des groupes cybercriminels majeurs et la prolifération de rançongiciels accessibles sur l'Internet sombre pour des cybercriminels disposant de faibles compétences sont trois causes majeures de l'augmentation de ce type d'attaque. La situation est aggravée par le faible niveau de sécurité des systèmes d'information des entités victimes et par l'absence de préparation de nombreuses entités à une crise d'origine cyber majeure (absence de stratégie de résilience adaptée à la menace, absence de plan de gestion de crise, absence de plan de continuité et de reprise d'activité et lacunes dans les systèmes de supervision et de sauvegardes).

Les cybercriminels opérant des rançongiciels cherchent par divers moyens à faire pression sur la victime pour qu'elle paye la rançon. A ce jour, l'incitation principale du paiement d'une rançon est la rupture d'activité induite par la séquestration des données. Toutefois depuis 2020, de plus en plus de cybercriminels appliquent le principe de « double extorsion » en exfiltrant des données parfois sensibles et en les publiant sur Internet si la victime ne paye pas, ce qui l'expose à une atteinte à l'image et à un défaut dans le respect du règlement RGPD. Aujourd'hui, certains groupes cybercriminels tentent de multiplier les appels téléphoniques aux dirigeants des entités victimes et alertent également les journalistes spécialisés afin d'augmenter la pression sur les dirigeants et l'atteinte à l'image de l'entité.

Il est à noter que des groupes d'activistes commencent à utiliser les attaques par rançongiciel pour un motif politique et non lucratif (cf. pression d'activistes indiens contre la réforme agricole).

3.2.2 Attaques indirectes

Face aux meilleures mesures de sécurité informatique mise en place par certaines entreprises et administrations sensibles, les attaquants s'orientent désormais vers la compromission de la chaîne de distribution logicielle de leurs cibles finales ou des réseaux de prestataires de services travaillant pour ces dernières. A ce jour, plusieurs opérations d'espionnage informatique ont ciblé des organisations dans plusieurs secteurs d'activité sensibles (santé, énergie ou secteurs détenteurs de propriété intellectuelle). Ainsi, à titre d'exemple, l'attaque sur la chaine de distribution logiciel de l'éditeur américain SOLARWINDS a permis la compromission de son produit *Orion*. Cette attaque aurait ensuite permis l'accès à de très nombreuses entités dans le monde, en particulier à des agences gouvernementales américaines.

3.2.3 Vulnérabilités critiques exploitées massivement par les cyberattaquants

Plusieurs vulnérabilités d'importance critique ont encore été dévoilées depuis le début de l'année 2021. En mars, MICROSOFT a ainsi indiqué que plusieurs vulnérabilités identifiées dans sa messagerie virtuelle *Microsoft Exchange* avaient été exploitées par des attaquants. Celles-ci permettent à un attaquant d'exécuter un code malveillant à distance, sans nécessité de s'authentifier. Elles ont fait l'objet d'une alerte auprès des OIV, OSE et ministères français.

L'éditeur a également publié un correctif de sécurité lors de sa mise à jour mensuelle pour de multiples vulnérabilités critiques concernant un mécanisme du serveur DNS qu'il propose. Dernièrement, une faille découverte dans le produit de sécurité et de contrôle d'accès *BIG-IP* de l'éditeur F5 NETWORKS permettrait d'exécuter à distance certaines actions dans les systèmes d'informations. Elle aurait été exploitée massivement par des attaquants.

4 [NP] Adaptation de la posture Vigipirate « été – automne 2021 »

La posture Vigipirate « *été – automne 2021* », active à compter du 19 juin 2021 , **maintient le territoire national au niveau « *sécurité renforcée - risque attentat* ».**

4.1. Sécurité des lieux de rassemblement et des lieux de culte

- *Contexte général*

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 sollicitée.

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 sus-cités. 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.

- *Objectifs de sécurité recherchés sur la période*
    - *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. En liaison avec les autorités religieuses locales, la mise en œuvre de mesures de contrôle des accès est recommandée.

    - *Mesures propres aux périodes de vacances scolaires*

Les lieux sujets à de fortes affluences saisonnières durant les vacances scolaires (salles de spectacles, plages, etc.) bénéficieront de moyens adaptés. Les services de l'État (forces de sécurité intérieure – unités Sentinelle) adapteront leur dispositif en conséquence. Les opérateurs seront incités à solliciter l'appui des référents sûreté départementaux de la police ou de la gendarmerie nationale.

    - *Guide des bonnes pratiques de sécurisation d'un événement de voie publique*

Le ministère de l'intérieur a publié et diffusé un Guide des bonnes pratiques de sécurisation d'un événement de voie publique en octobre 2018. Il est disponible sur le site Internet du ministère de l'Intérieur : https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Securisation-des-evenements-de-voie-publique.

4.2. Sécurité des grands espaces de commerce, de tourisme et de loisir

- *Contexte général*

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

La sécurité sera renforcée autour des grands espaces de rassemblements ayant pour objet des activités commerciales (salons d'expositions, foires, etc.), les interconnexions de transports en milieu clos dotées de commerces (métros, gares, etc.) demeureront également un point de vigilance.

Cette période de réouverture potentielle appelle une vigilance accrue notamment sur le secteur du tourisme et des parcs de loisirs, particulièrement fréquentés au moment des vacances scolaires. Enfin, la sécurité des grands espaces de commerce lors des soldes d'été, marquées par une forte affluence, demeure un axe d'attention majeur.

De façon plus générale, il revient aux autorités préfectorales d'évaluer le niveau de de menace pour les différentes activités sises dans leur département. Lorsque des éléments objectifs attestent d'une menace sur le plan local, ou qu'un événement révèle une vulnérabilité particulière, ceux-ci sont communiqués aux responsables de sûreté des établissements concernés afin de leur permettre d'adapter leur dispositif, le cas échéant avec la mise en œuvre de mesures de protection et de contrôle spécifiques décidées par l'autorité préfectorale.

Cette démarche s'inscrit dans la volonté de renforcer les liens et la coordination entre acteurs publics et privés.

- *Objectifs de sécurité recherchés sur la période*

La sécurisation des grands espaces de commerce, des sites de tourisme et de loisirs passe, entre autres, par :

    - *La sensibilisation des personnels :*

Elle doit être assurée par les gestionnaires de centres et d'enseignes commerciaux.

Les salariés doivent avoir été sensibilisés aux comportements à adopter en cas de situation suspecte, de menace d'attaque terroriste, de confinement ou d'évacuation. Ils doivent également avoir été informés de la procédure de signalement des comportements suspects en vigueur dans leur établissement. Par ailleurs, les responsables d'enseignes sont incités à former leur personnel aux gestes de premiers secours.

La connaissance fine des sites par le personnel qui y travaille et l'organisation d'exercices collectifs constituent des prérequis indispensables.

- *Le renforcement des échanges et de la coordination entre acteurs publics et privés :*

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

Pour rappel, la convention nationale, signée le 19 février 2019, entre le secrétaire d'Etat auprès du ministère 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 à ces établissements de mettre en place un plan de sûreté et de désigner 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 nouvelle dynamique d'échanges d'informations. Le développement de ces conventions locales est recherché.

- *Un dispositif de détection du 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.

Sur la voie publique, la vidéoprotection peut être mise en œuvre 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 (Cf. art. L. 223-1 du code de la sécurité intérieure).

Il est souhaitable que les préfets accordent aux espaces de commerce, dans toute la mesure du possible, l'extension de leur vidéosurveillance aux abords immédiats de la voie publique. Par ailleurs, pour les espaces complexes le justifiant[1], le recours à la notion de « périmètre vidéoprotégé » peut-être utilement envisagé.

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

4.3. Sécurité des transports collectifs

- *Contexte général*

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, événements sportifs ou festifs, etc.). A ces occasions, le niveau de sécurité des plateformes aéroportuaires, des gares, des ports et des réseaux de transport en commun doit être renforcé[2].

- *Objectifs de sécurité recherchés sur la période*
  - *Espaces d'accueil des voyageurs pour tout mode de transport*

La menace visant les emprises des gares, des aérogares et des stations de métro ou de RER impose une vigilance quotidienne. Les couloirs de liaison intermodaux doivent faire l'objet d'une attention particulière.

  - *Spécificité du transport aérien*

Même si la pandémie impacte la fréquentation 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'Etat et les opérateurs poursuivront l'amélioration de la sécurisation du côté ville.

---

[1] Chapitre 1er du décret n°96-926 du 17 octobre 1996 relatif à la vidéoprotection pris pour application des articles 10 et 10-1 de la loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité et modifié par décret n°2012-112 du 27 janvier 2012, art4.

[2] L'efficacité des mesures de contrôle dans les transports peut être accrue par le rappel des dispositions tirées des lois SAVARY, URVOAS et LEROY de 2016.

Une coordination étroite entre les FSI, 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.

- *Infrastructures et réseaux ferroviaires*

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 à grande vitesse, réseaux interurbains, etc.) doit faire l'objet d'une communication immédiate aux FSI 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 ;
- **mèl** : permanence.cmvoa@developpement-durable.gouv.fr

➢ *Transport maritime de passagers*

Il est recommandé aux exploitants portuaires et aux armateurs d'assurer la continuité du contrôle des véhicules, de leurs passagers et de leur chargement. Conformément à l'arrêté du 16 juillet 2018, modifiant l'arrêté du 4 juin 2008[3], relatif aux conditions d'accès et de circulation en zone d'accès restreint des ports et des installations portuaires et à la délivrance des titres de circulation. A ce titre, tout armateur exploitant des navires rouliers à passagers mettra en place un dispositif destiné à prévenir l'introduction des articles prohibés (armes à feu, explosifs, etc.), par les personnes en sortie des espaces rouliers, au moment de leur accès aux espaces publics du navire.

L'effort de ciblage, reposant sur l'analyse et la détection de comportements particuliers avant l'embarquement, en liaison avec les autorités portuaires (enregistrement tardif, véhicule de location, personne seule dans le véhicule, etc.), est reconduit.

Sous l'autorité des préfets maritimes, le déploiement aléatoire d'équipes de protection constituées d'agents de l'Etat, à bord des navires à passagers sous pavillon français à destination des îles métropolitaines, dont notamment la Corse, ainsi qu'à destination du Royaume-Uni reste en vigueur. En cas de menace avérée, le déploiement de ces agents est également possible à bord des navires à passagers sous pavillon français à destination de l'Algérie et de la Tunisie.

Afin de protéger le trafic maritime d'intérêt, l'incitation à adhérer à la coopération navale volontaire doit être poursuivie, auprès des armateurs français et étrangers, comme auprès des opérateurs terrestres qui font appel à des services maritimes. L'annexe 4 présente succinctement le dispositif de la CNV ainsi que les zones actives de mise en œuvre.

Conformément à la mesure MAR 12-02, l'application du niveau 2 du code ISPS est maintenue dans les zones suivantes : au Nord-ouest de l'Océan indien, dans le Golfe arabo-persique, dans la zone comprise entre les mers de Sulu et Célèbes (espace compris entre le nord de l'Indonésie et les Philippines), dans les détroits de Malacca et de Singapour et dans les ports de Libye. Dans le Golfe de Guinée, compte tenu de la recrudescence des actes de piraterie, et de l'évolution de leur répartition géographique, la zone d'application du niveau 2 est étendue jusqu'à 250 Nq des côtes.

4.4. Sécurité des bâtiments publics

➢ *Contexte général et objectif de sécurité recherché sur la période*

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

Des mesures renforcées de sécurité seront mises en place dans et aux abords des commissariats et des brigades de gendarmerie, notamment s'agissant des accueils.

Il convient d'actualiser les annuaires de crise au sortir de la période estivale et les procédures d'alerte afférentes de même que les plans de protection et les procédures internes d'évacuation ou de confinement seront portés à la connaissance des nouveaux arrivants.

Une vigilance particulière sera également portée aux bureaux de vote pendant la durée des élections mais aussi à la sécurité des palais de justice et des établissements pénitentiaires dans le contexte de procès dits « sensibles ». Elle sera renforcée lors des procès des personnes mises en cause pour faits de terrorisme. La sécurisation des juridictions abritant ces occurrences constituera un axe d'effort spécifique.

[3] En application de cet arrêté modificatif, la fiche MAR 10-03 a été créée et ajoutée au plan gouvernemental VIGIPIRATE.

Cette vigilance peut également concerner **les sites de la protection judiciaire de la jeunesse**, qui prend en charge des mineurs poursuivis pour association de malfaiteurs à but terroriste.

4.5. Sécurité des établissements scolaires, de l'enseignement supérieur et de l'enseignement technique agricole ainsi que des structures d'accueil collectif de mineurs (ACM) à caractère éducatif

- *Contexte général*

Dans un contexte où l'état de la menace terroriste demeure à un niveau très élevé, les établissements et services rattachés au ministère de l'éducation nationale, de la jeunesse et des sports et au ministère de l'enseignement supérieur, de la recherche et de l'innovation (MENJS/MESRI) doivent maintenir la plus grande vigilance. L'attentat perpétré le vendredi 16 octobre 2020 à Conflans-Sainte-Honorine à l'encontre d'un professeur a rappelé le caractère très sensible de ces derniers.

La typologie de la population accueillie, la physionomie des bâtiments, mais également les caractéristiques des dernières attaques terroristes sont autant de facteurs confirmant la nécessité de maintenir à un niveau élevé les mesures de sécurisation déployées.

Par ailleurs, la fin de l'année scolaire 2020-2021, la passation des examens dont les modalités ont été adaptées au contexte sanitaire, la promulgation des résultats des examens et concours de fin d'année, les séjours de cohésion dans le cadre du service national universel, les activités estivales des structures d'accueil collectif de mineurs (ACM) et des universités, la préparation finale des sportifs de haut-niveau en vue des jeux Olympiques et Paralympiques de Tokyo, ainsi que la rentrée scolaire 2021-2022 constituent autant de vulnérabilités sur la période couverte.

A ce titre, les établissements et les services administratifs des MENJS/MESRI doivent maintenir un haut niveau de protection et développer une culture commune de gestion de crise dont l'un des objectifs est d'accroître l'interopérabilité avec les services préfectoraux, les forces de sécurité intérieure et les collectivités locales.

Les services et les établissements des MENJS/MESRI prendront donc toutes les dispositions jugées nécessaires pour se prémunir contre les menaces identifiées. Ils participent activement à la mise en œuvre opérationnelle des politiques publiques en matière de protection des populations, en s'appuyant sur les directives interministérielles[4]. La complémentarité des actions au sein de l'appareil de gestion de crise décliné à l'échelon territorial est fondamentale, et sera systématiquement recherchée.

- *Objectifs de sécurité recherchés sur la période*

▪ Reconduction des principales mesures VIGIPIRATE

Au regard du caractère sensible des établissements relevant des MENJS/MESRI, il est demandé de maintenir un niveau élevé de sécurisation et de contrôle des flux de personnes. Une attention particulière sera portée aux rassemblements organisés au sein et/ou aux abords des établissements, notamment à l'occasion de la fin d'année scolaire et universitaire 2020-2021 et de la prochaine rentrée scolaire et universitaire 2021-2022 ainsi que lors d'événements sportifs, de colloques, conférences, rencontres scientifiques, de déplacements en groupe sur le temps scolaire et hors du temps scolaire, y compris lors des activités organisées par les ACM.

Dans cette perspective, bien que l'obligation du port du masque constitue une nécessité sanitaire et une obligation réglementaire qui peut rendre plus difficile le contrôle visuel, il est impératif de maintenir une surveillance active, un contrôle des accès aux différents sites et emprises bâtimentaires, et un filtrage des flux.

Enfin, dans l'hypothèse de déplacements à l'étranger, le respect des consignes diffusées par le ministère de l'Europe et des affaires étrangères est de rigueur, ainsi que le renseignement et l'utilisation de l'application Ariane par l'ensemble des personnels relevant des MENJS/MESRI et les structures organisatrices.

▪ Sécurisation des personnes et des biens, plan de continuité/reprise d'activité

L'élaboration et/ou la mise à jour des plans particuliers de mise en sûreté (PPMS) « attentat-intrusion », ainsi que la réalisation des exercices annuels associés doivent impérativement être menés à bien par les écoles et établissements scolaires. Le déploiement des diagnostics de mise en sûreté doit se poursuivre.

[4] Instruction relative au renforcement des mesures de sécurité et de gestion de crise applicables dans les écoles et les établissements scolaires du 12 avril 2017.

En outre, il est nécessaire de poursuivre l'élaboration et/ou la mise à jour des plans de continuité d'activité et des dispositifs de gestion de crise des services déconcentrés.

Pour les établissements d'enseignement supérieur et de recherche, la mise en œuvre du « plan de sécurisation ESRI », en collaboration étroite avec les forces de sécurité intérieure qui pourront être sollicitées dans cette perspective, demeure une priorité.

L'ensemble des intervenants des chaines de sécurité identifiées veilleront à remonter toute situation pouvant devenir problématique au service compétent.

Pour les ACM, le renforcement de la surveillance des accès aux accueils (accueils de loisirs, séjours de vacances et camps scouts) et la mise en œuvre des bonnes pratiques de prévention figurant dans le « guide à destination des organisateurs, des directeurs et des animateurs en charge d'accueils collectifs de mineurs à caractère éducatif » doivent être recherchés. Dans les établissements et les sites des opérateurs sous tutelle des MENJS/MESRI et du MAA, une attention particulière sera portée à la protection et aux contrôles des lieux abritant des matériels et des produits toxiques. De manière générale, les zones considérées comme « sensibles », (zones à régime restrictif, zones sécurisées, zones d'accès restreint.), doivent faire l'objet d'une vigilance maximale et de la mise en place de procédure de contrôle renforcées, le cas échéant conformément aux dispositions réglementaires spécifiques applicables.

- **La sécurisation des systèmes d'information (données et infrastructures physiques)**

Il est demandé aux services et établissements des MENJS/MESRI de veiller :

- au respect de la politique de sécurité des systèmes d'information de l'Etat (PSSIE) afin de satisfaire aux exigences de cyber sécurité, qui doit être considérée comme prioritaire face au déploiement du télétravail et à la recrudescence des cyberattaques,
- à l'application du guide d'hygiène informatique de l'agence nationale de la sécurité des systèmes d'information (ANSSI)[5],
- à la protection au niveau adéquat des locaux dédiés à l'installation des systèmes d'information, des stockages de données et des systèmes de restauration,
- à l'utilisation de systèmes d'information présentant un niveau de sécurité compatible avec la note ministérielle HFDS N°2020-0363 du 21/07/2020 relative aux « modalités de souscription à des offres de services d'informatique en nuage », le guide précité d'hygiène informatique de l'ANSSI, ainsi que les dispositions relatives au règlement général sur la protection des données (RGPD) en visant notamment la protection des données personnelles.

- **Une collaboration étroite entre les acteurs de la gestion de crise au plan local**

Afin de contribuer pleinement à l'action coordonnée de l'ensemble des administrations, établissements, et opérateurs dans les territoires au regard des problématiques de sûreté, de sécurité, d'anticipation et de gestion de crise, une approche partenariale visant à renforcer les mesures de protection des personnes et des biens, doit guider ces actions. Une culture partagée de la sûreté et de la sécurité est recherchée. Le partage d'informations entre les différents acteurs doit se traduire concrètement par :

- la participation des différents acteurs aux projets de sécurisation des services, établissements et organismes,
- la participation aux réunions d'état-major de la sécurité et aux exercices ministériels et/ou interministériels de gestion de crise.
- le déploiement de procédures partagées des chaines d'alerte et de gestion de crise,
- la mise à jour des annuaires interministériels des acteurs de la gestion de crise
- la communication aux partenaires des PPMS « attentat-intrusion » (ou leur équivalent pour les établissements relevant de l'ESRI) et des plans des bâtiments actualisés,
- la mise en œuvre d'exercices communs.

[5] https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

Les points énumérés ci-dessus n'excluent en rien les autres actions qui peuvent être entreprises dans ce même esprit, y compris en élargissant cette posture à d'autres secteurs ministériels. Ces derniers ont d'ailleurs toute latitude pour s'appuyer sur les orientations et réflexions des MENJS/MESRI/MAA en ce domaine.

4.6. Sécurisation des sites touristiques, culturels et des expositions à thème sensible

La réouverture des sites culturels et touristiques après parfois plusieurs mois de fermeture appelle à renouveler les messages de vigilance habituels. Les exploitants de sites, d'événements et d'établissements culturels sont invités à réviser leurs procédures de sûreté afin de s'assurer que les salariés et agents chargés de cette mission bénéficient du niveau de préparation adapté à un haut niveau de menace terroriste. Plusieurs documents élaborés pour soutenir les responsables de sites ou d'événements peuvent être consultés sur le site Internet du ministère de la Culture : http://www.culture.gouv.fr/Actions-de-renforcement-et-de-surveillance-des-lieux-culturels. Cette documentation doit permettre la réalisation d'exercices dans la perspective de valider les procédures internes de confinement ou d'évacuation en cas d'attaque directe ou à proximité.

La persistance probable des contraintes liées à la crise sanitaire ne doit pas conduire à baisser la garde. Il est conseillé aux responsables d'établissements de reprendre les contacts avec les forces de sécurité intérieure (police nationale et gendarmerie nationale) afin de leur présenter les conditions d'accueil du public et les évolutions éventuelles de jauge et de procédures.

Compte tenu des sinistres récents, les établissements culturels sont invités à compléter ou à mettre à jour leur plan de sauvegarde des biens culturels (PSBC). La protection du patrimoine culturel compte parmi les objectifs du dispositif ORSEC, le PSBC doit donc être réalisé en relation étroite avec les services de secours et être mis à leur disposition en cas d'intervention.

4.7. Sécurité des établissements de santé, sociaux et médico-sociaux

- *Contexte général*

Les établissements de santé, sociaux et médico-sociaux, par nature ouverts sur l'extérieur, demeurent des cibles particulièrement vulnérables. La vigilance doit donc rester élevée particulièrement pour les établissements de santé, médico-sociaux et pour les sites de production, de stockage et de distribution de produits de santé (masques, EPI..).

- *Objectifs de sécurité recherchés sur la période*

Les préfectures veillent au maintien des actions mises en œuvre par les forces de sécurité intérieure :

- la sécurisation des abords des établissements de santé de niveau 1 (selon la cartographie transmise par les ARS) ;
- 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 de l'effectivité de la mise en œuvre des mesures de sûreté de leur plan de sécurisation d'établissement (PSE). Ils poursuivent les actions de formation à destination de leurs personnels et s'attachent à s'assurer de leur efficacité.

Les responsables des établissements et des services sociaux et médico-sociaux (ESSMS), poursuivent le déploiement de leur stratégie de protection, en suivant les recommandations du ministère des solidarités et de la santé.

Point d'attention :

- la sécurisation des centres de prélèvement ou de vaccination, conformément aux recommandations émises par le ministère ;
- les opérateurs d'importance vitale doivent faire l'objet d'une vigilance toute particulière au regard de la crise sanitaire actuelle. Les sites de production de médicaments (vaccins, hydroxychloroquine) méritent également la mise en œuvre de mesures de sécurisation adaptées.

- *Cyber sécurité des structures de santé*

La recrudescence des cyberattaques par rançongiciel qui ont affecté fin 2020 et début 2021 les établissements de santé nécessite que la protection cyber soit encore renforcée. En coordination avec l'ANSSI, le ministère des solidarités et de la santé a pris de nouvelles mesures, dans le cadre du « Plan de renforcement de la cybersécurité des établissements de santé ». En cohérence avec les objectifs de cybersécurité recherchés sur la période par l'ANSSI (cf. § 4.9. « Sécurité du

numérique), ces mesures portent en particulier sur l'identification et la correction des vulnérabilités affectant les infrastructures réseau et les postes de travail et sur la sécurisation des dispositifs de sauvegarde.

Une attention particulière doit être portée :

- aux établissements de santé opérateurs d'importance vitale et opérateurs de services essentiels, dont le maintien des capacités de soins conditionnent la réponse sanitaire dans les territoires, notamment en cas d'évènements exceptionnels graves ;
- aux établissements ultramarins, du fait des risques induits par leur isolement géographique ;
- à la chaîne vaccinale contre la COVID-19.

4.8. Protection des ressortissants et intérêts français à l'étranger (IFE)

➢ *Contexte général*

A l'étranger, la France peut être directement menacée par des organisations terroristes.

La circulaire du Premier ministre n°5777/SG du 26 mars 2015 définit le rôle capital de l'Ambassadeur pour assurer la sécurité des agents et des implantations de la France à l'étranger.

L'augmentation de la menace terroriste pouvant viser directement les agents de l'Etat et des opérateurs du MEAE à l'étranger, ainsi que les implantations étatiques françaises est prise en compte.

Cette évaluation de la menace définit également les mesures à prendre pour assurer la sécurité de la communauté française et des touristes français.

➢ *Objectifs de sécurité recherchés et acteurs concernés*

L'Ambassadeur avec l'appui des responsables des services de l'Etat et des opérateurs procède à une analyse des risques potentiels et propose une stratégie de sécurité qui porte à la fois sur les actions à mettre en place et les mesures préconisées pour le renforcement de la sécurité des agents et des implantations.

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

- *Information et sensibilisation*

Edition des « *Conseils aux voyageurs* », régulièrement mise 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.

Réponse téléphonique active (24/7).

- *Formation des agents des postes diplomatiques et consulaires à la gestion de crise et aux accidents collectifs*
- *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.

Elaboration de plans d'urgence destinés à organiser la prise en charge de victimes françaises.

Suivi des familles de 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'Etat portent sur les mesures de sécurité active et passive ainsi qu'organisationnelles. Elles incluent des volets de formation renforcée, notamment des exercices de confinement/évacuation, de formation « *Comment réagir à la réaction en cas d'attaque armée* » et de formations longues « *Départ en postes sensibles* ».

4.9. Sécurité du numérique

➢ *Contexte général*

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

➢ *Objectifs de sécurité recherchés sur la période*

L'évaluation de la menace pour la sécurité du numérique présentée aux paragraphes supra nécessite d'appliquer les objectifs et mesures de sécurité suivants :

- Mesure NUM 11-02 - Rechercher sur le SI des marqueurs particuliers correspondant à une attaque :
    - Compte tenu des campagnes d'exploitation des vulnérabilités SolarWinds et Microsoft Exchange, il est recommandé de prendre connaissances des marqueurs de vulnérabilités via les rapports des éditeurs de sécurité et indiquer à l'ANSSI le résultat de la recherche et ses modalités, même si elle est négative.

- Mesure NUM 31-09 - Rappeler l'importance d'une mesure d'hygiène ou sectorielle existante :
    - Pour sécuriser les accès à distance des systèmes d'information en cas de télétravail, il est recommandé de recourir à une authentification forte, afin d'éviter une authentification depuis un poste attaqué, volé ou perdu et s'assurer du caractère sécurisé de la connexion réseau à travers Internet lorsqu'un utilisateur a besoin de se connecter au système d'information de l'entité à distance. Au regard des menaces d'attaque par hameçonnage, il importe de sensibiliser les utilisateurs à être particulièrement attentifs aux courriels qu'ils reçoivent, les inciter à ne pas activer les macros dans les pièces jointes et réduire l'exécution des macros. La fiche « hameçonnage » du SGDSN est une ressource utile: http://www.sgdsn.gouv.fr/vigipirate/securite-du-numerique-lhameconnage-ou-phishing/.

- Mesure NUM 41.01 - Valider et appliquer un correctif de sécurité :
    - Face aux vulnérabilités critiques, il est important d'appliquer les correctifs de sécurité mentionnés dans les bulletins d'alerte du CERT-FR disponibles sur le site www.cert.ssi.gouv.fr. Sur le même site, des avis de sécurité correspondant à la veille sur plus d'une centaine de produits est aussi effectués.

- Mesure NUM 41.02 - Vérifier la correction effective d'une vulnérabilité :
    - Face aux récentes vulnérabilités affectant Microsoft Exchange, l'ANSSI souhaite contrôler le niveau de sécurité et notamment des annuaires Active Directory de chaque Opérateur d'Importance Vitale, Opérateur de Services Essentiels et de chaque ministère. A cette fin, l'ANSSI conseille d'utiliser l'outil de collecte en source ouverte ORADAD (Outil de récupération automatique de données de l'Active Directory).

- Mesure NUM 51-02/52-02 - Adapter les dispositifs de réponse à incidents aux caractéristiques de la menace :
    - Compte tenu de la menace persistante liée aux rançongiciels, il est essentiel de s'assurer que les outils et dispositifs de réponse à incident sont opérationnels et adaptés à la menace numérique et que le personnel chargé de le mettre en œuvre soit familiarisé avec celui-ci. Il est par ailleurs recommandé d'effectuer un exercice d'activation du PCA ou de gestion de crise cyber si le dernier exercice a été effectué il y a plus d'un an. Le guide de l'ANSSI sur les exercices de gestion de crise cyber aide les entités à organiser ces exercices : https://www.ssi.gouv.fr/guide/organiser-un-exercice-de-gestion-de-crise-cyber/.

- Mesure NUM 51-06 - Procéder régulièrement à un séquestre hors ligne exceptionnel des sauvegardes des systèmes les plus critiques :
    - En cas d'attaque par rançongiciel et de destruction ou d'altération des données, il est important de pouvoir restaurer le bon fonctionnement des systèmes les plus critiques en s'assurant que les éléments sauvegardés ne soient pas accessibles par un quelconque réseau, y compris avec des comptes d'administration. Le guide de l'ANSSI « Attaques par rançongiciels, tous concernés - Comment les anticiper et réagir en cas d'incident ? » aide les entités à réduire le risque d'attaque et réagir lorsque celle-ci réussie : https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf/.

5 Consignes particulières de vigilance, prévention et protection

5.1. 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. Elles seront sensibilisées et informées par leurs autorités de tutelle des mesures de sécurité à appliquer.

5.2. 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 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 véhicule-bélier* », disponible sur le site Internet du SGDSN : http://www.sgdsn.gouv.fr/vigipirate ;
- le guide du ministère de l'intérieur évoqué au § 4.1.

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

Les récents attentats, ou actes de malveillance, commis en Europe, ont démontré une capacité à fabriquer des explosifs artisanaux ou des substances toxiques à partir de produits chimiques d'usage courant. Les professionnels qui vendent ce type de produits 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 – 01 78 47 34 29 (24/7).

5.4. [DR] Rappels des consignes NRBC aux services intervenants

En cas d'attaque NRBC, il est déterminant que les services intervenants mettent en œuvre, sans délai, les moyens, procédures et protocoles afin d'en minimiser les effets.

Pour cela, il se révèle indispensable de :

- contrôler la diffusion et la connaissance des consignes NRBC auprès des agents qui auraient à les mettre en œuvre (fiches réflexes, instructions et circulaires, participation aux formations et entraînements interministériels) ;
- rappeler les consignes de protection et les conduites à tenir individuelles et collectives ;
- déplacer, si nécessaire, certains moyens NRBC vers les sites de grands rassemblements du public : lots PRV NRBC, unités mobiles de décontamination. En cas de déplacement de ces moyens NRBC, il est nécessaire, dans cette zone, d'activer la fiche ALR 22.05 (assurer la disponibilité des tenues de protection et moyens NRBC dans les véhicules des services de secours et d'aide médicale d'urgence, ainsi qu'auprès des personnels de la police, de la gendarmerie ou des unités militaires amenées à intervenir).

5.5. Sensibilisation à la lutte anti-drone

L'utilisation des drones est un mode d'action régulièrement mis en œuvre pour capter des images ou diffuser des messages[6] mais qui peut évoluer vers des actes de malveillance ou terroristes. A l'occasion de grands rassemblements, les organisateurs doivent prendre en compte cette menace en sollicitant l'avis des référents sûreté locaux de la police ou de la gendarmerie nationales.

6 Sensibilisation du grand public

Malgré la crise sanitaire actuelle, le niveau élevé de la menace exige le maintien d'une vigilance accrue.

6.1. Efforts de communication

[6] Comme lors d'un match de football au Luxembourg le 3 octobre 2019.

Les ministères veilleront à ce que les opérateurs publics et privés situés dans leur champ de compétence mettent en place les logogrammes **: « *Sécurité renforcée - risque attentat* ».**

Ces logogrammes peuvent être téléchargés sur le site :

- du Gouvernement http://www.gouvernement.fr/vigipirate ;
- du SGDSN http://www.sgdsn.gouv.fr/vigipirate .

Les ministères et les préfets sont invités à relayer le plus largement possible les outils de sensibilisation à la menace terroriste téléchargeables sur les deux sites cités *supra*.

6.2. Sensibilisation des professionnels et du grand public aux bonnes pratiques

Dans un souci de large diffusion des bonnes pratiques face à la menace terroriste, figurent en annexe des fiches de sensibilisation à destination, tant du grand public que des professionnels. Ces fiches renouvelées sont accessibles en ligne depuis l'espace Vigipirate du site Internet du SGDSN.

Elles sont également sur l'espace dédié du site du Gouvernement : http://www.gouvernement.fr/risques/le-citoyen-au-coeur-du-nouveau-dispositif-vigipirate.

La communication des mesures et des comportements à adopter en cas d'attaque terroriste au sein des établissements et lieux recevant du public doit être renforcée. Elle peut se faire par le biais de l'affiche « *Réagir en cas d'attaque terroriste* ». Cette affiche, qui peut être téléchargée sur le site du gouvernement (http://www.gouvernement.fr/reagir-attaque-terroriste), ainsi que sur le site du SGDSN, doit être imprimée sur un format adapté au lieu où elle est placée et visible du public (privilégier les entrées et sorties des établissements, les halls, ou salles d'attente, etc.).

En complément de ce dispositif, le *service d'information du gouvernement* (SIG) vient de diffuser une affichette intitulée « *Les gestes d'urgence si quelqu'un a été blessé autour de vous* ». Elle délivre des messages simples et concis pour expliquer comment faire un garrot, comment faire cesser les saignements, ou encore comment prendre en charge une personne ayant perdu connaissance, en attendant l'arrivée des secours.

L'affichette est diffusée sur les réseaux sociaux et peut-être téléchargée sur : http://www.gouvernement.fr/reagir-attaque-terroriste.

Par ailleurs, un ensemble de guides de bonnes pratiques, à destination des professionnels et des particuliers, est mis à disposition sur les deux sites précédemment cités.

La version publique du plan Vigipirate « *Faire Face Ensemble* », également disponible en langue anglaise, peut y être téléchargée.

Enfin, le SGDSN a développé, en liaison avec de nombreux partenaires, une plateforme de sensibilisation VIGIPIRATE qui se veut un outil pédagogique accessible au plus grand nombre.

Cette plateforme s'appuie en particulier sur le document « *Faire Face Ensemble* » de 2016 mais aussi sur les guides de bonnes pratiques destinés aux professionnels.

Elle intègre 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.

Elle 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.

ANNEXES

Annexe 1 : Cartographie des attentats djihadistes aboutis, déjoués en Europe de 2020 au 09 juin 2021 .
Diffusion sans restriction.

Annexe 2 : Historique des attentats djihadistes aboutis et déjoués en France de 2015 au 30 septembre 2020
Diffusion sans restriction.

Annexe 3 : Drones : Règles d'utilisation et mesures de prévention face à un usage malveillant
Diffusion sans restriction.

Annexe 4 : Zone de contrôle naval volontaire.
Diffusion sans restriction.

Annexe 5 : Fiche pratique prévention et signalement des cas de radicalisation djihadiste.
Diffusion sans restriction.

Annexe 1

Attentats djihadistes aboutis et déjoués en Europe en 2020 et 2021 (au 09/06/2021)

Aboutis

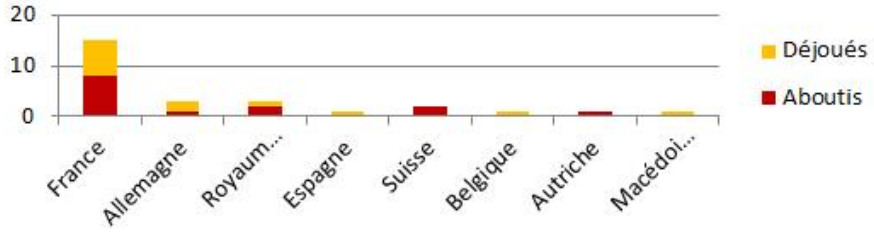
France (7)
Villejuif (03/01/20)
Romans-sur-Isère (04/04/20)
Colombes (27/04/20)
Paris (25/09/20)
Eragny (16/10/20)
Nice (29/10/20)
Rambouillet (23/04/2021)

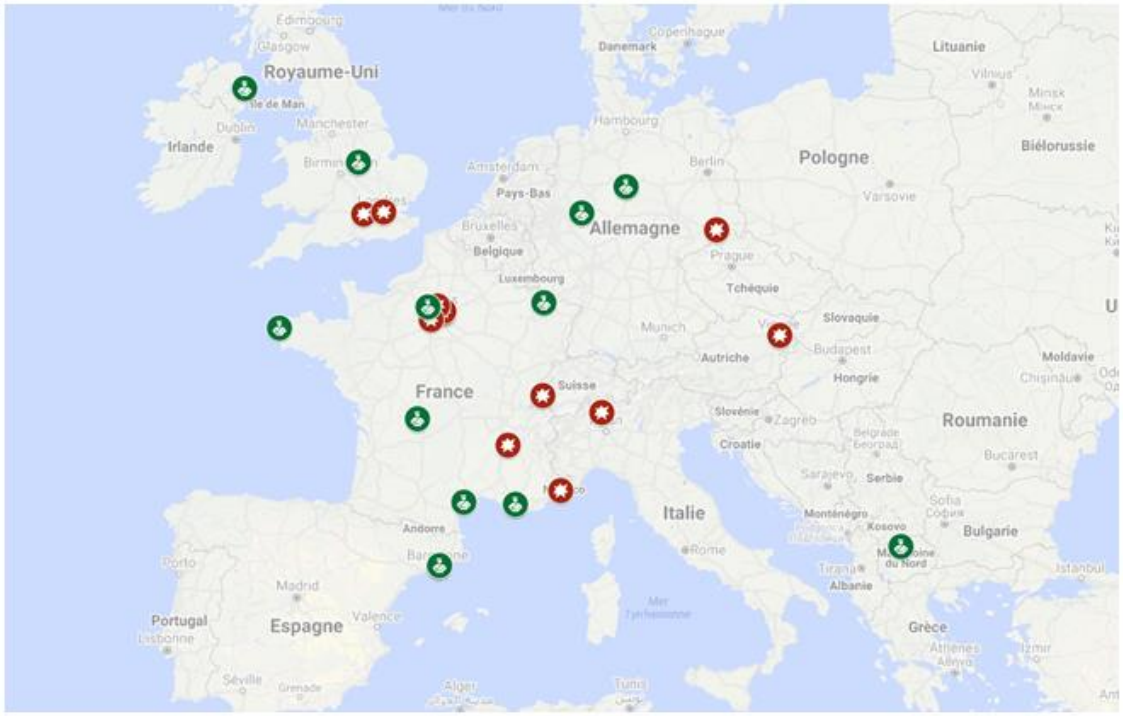
Royaume-Uni (2)
Londres (02/02/20)
Reading (20/06/20)

Allemagne (1)
Dresde (04/10/20)

Suisse (2)
Morges (12/09/20)
Lugano (24/11/20)

Autriche (1)
Vienne (02/11/20)





Déjoués

France (5)
Brest (20/01/20)
Moselle (27/10/20)
Mantes la Jolie (10/03/2021)
Marseille (10/03/2021)
Béziers (04/04/2021)

Allemagne (2)
Rhénanie du Nord-Westphalie (15/04/20)
Hesse (06/02/2021)

Royaume-Uni (1)
Londres & Leicester (09/07/20)

Espagne (1)
Barcelone (08/05/20)

Macédoine du Nord (1)
Skopje (01/09/20)

Hongrie (1)
Kecsemet (01/06/2021)

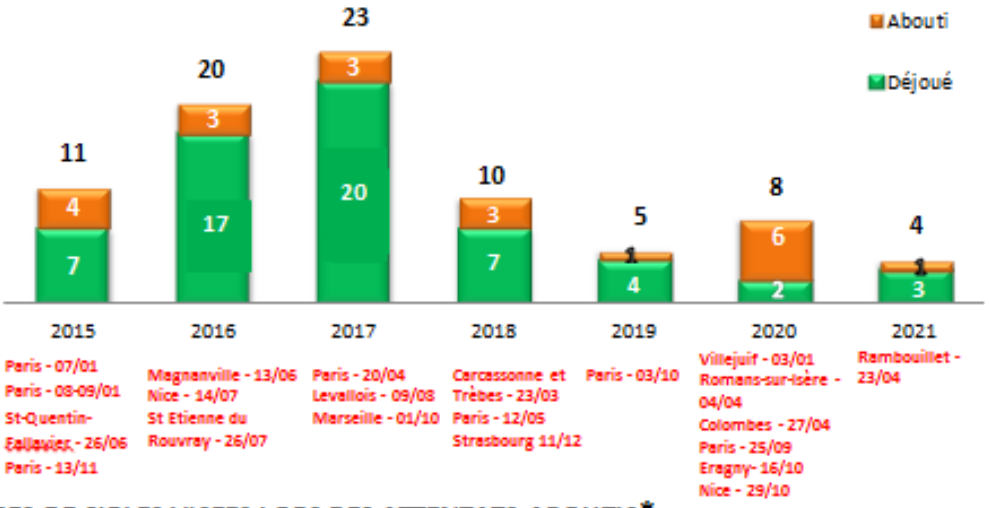
Norvège (1)
Oslo (04/02/2021)

***Attentats aboutis**: attentats mortels ou qui ont obtenu l'effet escompté par leur(s) auteur(s).*
***Attentats déjoués**: qui n'ont pu être menés à leur terme en raison de l'intervention des services de sécurité, et dont les protagonistes sont poursuivis judiciairement.*

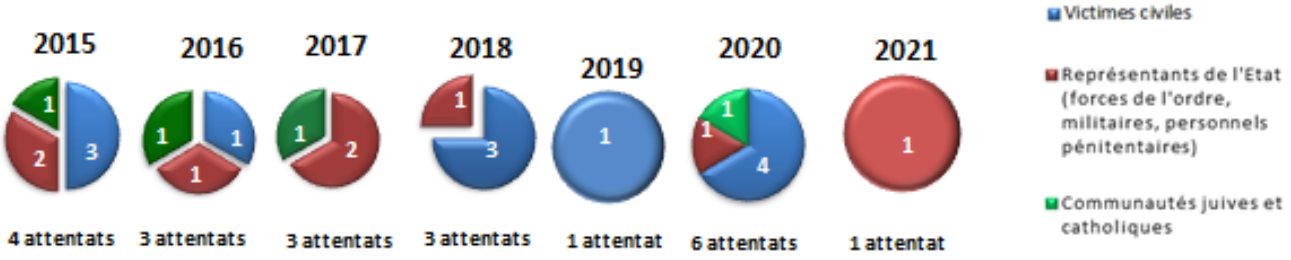
Annexe 2

HISTORIQUE DES ATTENTATS DJIHADISTES EN FRANCE DE 2015 A 2021
(au 09/06/2021)

RECAPITULATIF DES ATTENTATS ABOUTIS OU DEJOUES



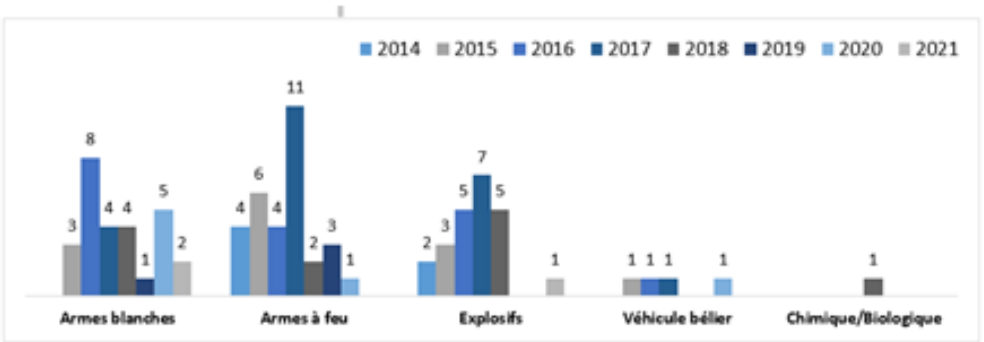
TYPES DE CIBLES VISEES LORS DES ATTENTATS ABOUTIS*



*plusieurs cibles ont parfois été visées lors d'un même attentat

Depuis 2015, les représentants en uniforme de l'autorité publique (forces de l'ordre, militaires, personnels pénitentiaires) sont les premières cibles visées par les assaillants lors d'attentats, suivies de la population civile : deux cibles relativement facilement atteignables. Si les cibles du terrorisme jihadiste visées pour leur appartenance religieuse étaient jusqu'à présent en baisse sur la période, le risque qui demeurait latent s'est fortement accru dernièrement.

MODES OPERATOIRES DES ATTENTATS ABOUTIS OU DEJOUES**



De façon générale sur la période les modes opératoires sommaires (utilisation d'armes par destination) demeurent les plus fréquemment utilisés (armes blanches, armes à feu, véhicule-bélier). Toutefois certains modes opératoires plus

**plusieurs modes opératoires ont parfois été utilisés ou envisagés lors d'un même attentat

Attentats aboutis : attentats mortels ou qui ont obtenu l'effet escompté par leur(s) auteur(s).
Attentats déjoués : attentats qui n'ont pu être menés à leur terme en raison de l'intervention des services de sécurité, et dont les protagonistes sont poursuivis judiciairement.

DRONES : RÈGLES D'UTILISATION ET MESURES DE PRÉVENTION FACE À UN USAGE MALVEILLANT

Fiche à l'attention des organisateurs de manifestations sur le domaine public

Elle précise les règles d'emploi des drones aériens de la gamme commerciale, tant pour un usage de loisir qu'une utilisation professionnelle, et liste les bonnes pratiques en matière de prévention contre les actes de malveillance pouvant être commis au moyen d'un drone.

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

1 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).

DRONES : RÈGLES D'UTILISATION ET MESURES DE PRÉVENTION FACE A UN USAGE MALVEILLANT

Fiche à l'attention des organisateurs de manifestations sur le domaine public

2 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.

3 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 oeuvre ;
- **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.

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

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

Maquette : Pôle graphique, fabrication, déplacements, imagerie – DSAF/DPSG – Juin 2021.

Annexe 4 : zone de contrôle naval volontaire.

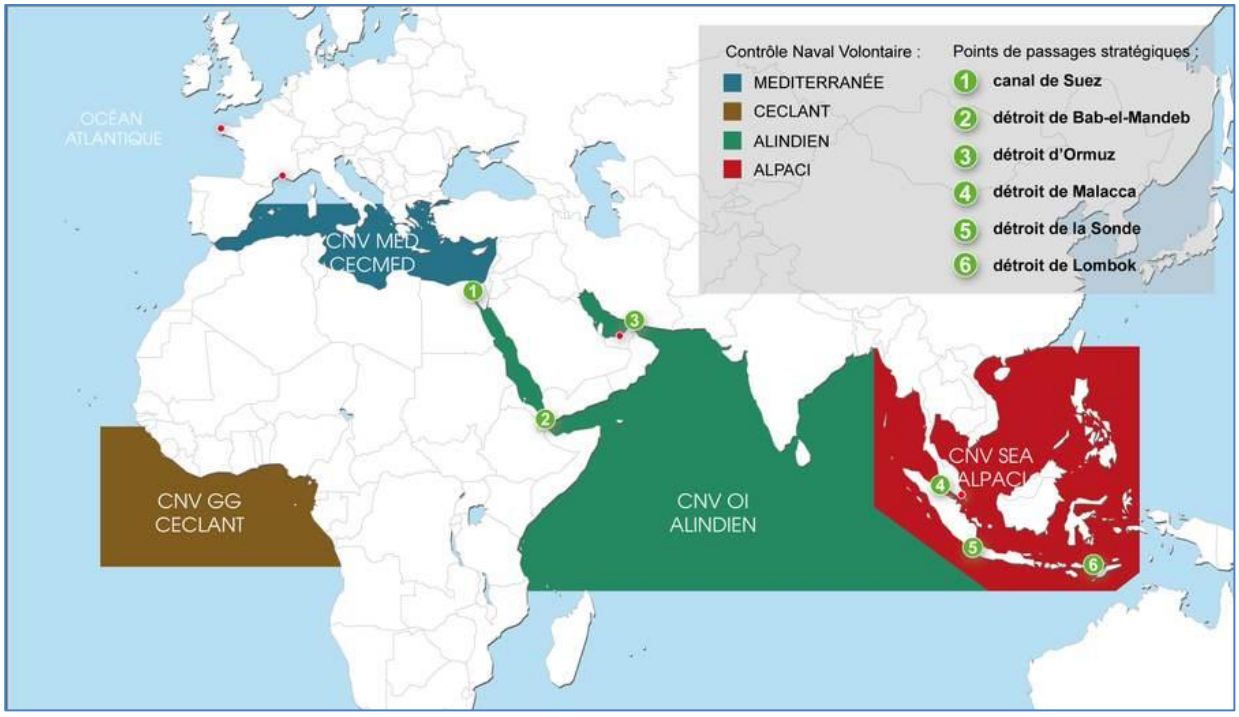
Diffusion sans restriction.

Objet de l'instruction interministérielle n°165/SGDS/PSE/PSN – n°100/SGMer du 29 avril 2019[7], la coopération navale volontaire (CNV) est une démarche volontaire entre les pouvoirs publics et les acteurs privés du monde maritime, favorisant le partage des informations dans le domaine de la sécurité et de la sûreté maritimes.

La CNV repose sur un réseau de capacités ministérielles et d'acteurs du monde maritime, au premier rang desquels figurent les armateurs français mais aussi les armements étrangers. Il est demandé aux administrations de promouvoir ce dispositif auprès des armateurs mais également auprès des opérateurs terrestres faisant appel à des services maritimes.

Les zones actives de CNV, reprises dans la mesure additionnelle MAR 11-01, sont précisées sur la carte ci-dessous :

- Zone Méditerranée ;
- Zone Golfe de Guinée ;
- Zone Océan indien ;
- Zone sud-est asiatique.



[7] Disponible sur le site du SGDSN www.sgdsn.gouv.fr

PRÉVENTION ET SIGNALEMENT DES CAS DE RADICALISATION

La radicalisation se caractérise par un changement de comportement qui peut conduire certaines personnes à l'extrémisme ou au terrorisme. L'objectif du signalement est de protéger ces personnes en les empêchant de commettre un acte criminel et de protéger la population de possibles comportements violents.

1 Pourquoi signaler un cas de radicalisation ?

La radicalisation **concerne tout type d'idéologie** qui peut conduire un individu à choisir l'action violente au nom de convictions auxquelles il adhère sans compromis possible. Cette action violente peut causer la mort d'autres membres de la société dont il rejette inconditionnellement les valeurs et le mode de vie.

Il s'agit d'un **processus de radicalisation** par paliers avec adhésion à une idéologie et rupture avec l'environnement habituel. La radicalisation apparaît comme un phénomène profondément lié à l'exploitation de conflits d'identité, de frustrations ou de fragilités. Certains groupes terroristes cherchent notamment à enrôler des individus en perte de repères et vulnérables.

La force d'une idéologie et son pouvoir d'attraction ne doivent pas être sous-estimés. Des individus ayant développé une haine de notre société peuvent adhérer pleinement à un discours qui donne sens à leurs frustrations ou sentiment d'humiliation.

La radicalisation est un phénomène complexe, amplifié par le développement des réseaux sociaux. La propagande véhiculée par des individus ou par des groupes touche des profils variés : délinquants, personnes vulnérables en quête d'identité, personnes ayant des troubles psychologiques ou psychiatriques, etc.

Difficile à repérer et à traiter, la radicalisation est donc un enjeu majeur de sécurité nationale.

2 Identifier une situation de radicalisation

Identifier un processus de radicalisation ne se fait pas sur la base d'un seul indice. Pris isolément, un des comportements listés ci-dessous ne signifie pas qu'il y a radicalisation. C'est la combinaison de plusieurs comportements contextualisés qui vous donne une forme de cohérence et qui doit provoquer votre étonnement.

COHÉRENCE → VIGILANCE → SIGNALEMENT

Les signaux de rupture :

- changements physiques et vestimentaires, alimentaires, de vocabulaire… inquiétants ;
- propos asociaux, apologie de la violence ;
- passage soudain à une pratique religieuse hyper ritualisée ou au contraire dissimulation manifeste ;
- rejet de l'autorité et de la vie en collectivité ;
- rejet brutal des habitudes quotidiennes ;
- repli sur soi ;
- expression de haine, discours complotistes, déplacement de la haine de soi sur autrui en raison d'une idéologie ;
- rejet de la société et de ses institutions (école, etc.) ;
- éloignement de la famille et des proches, fréquentation d'autres personnes radicalisées ;
- modification soudaine et inhabituelle des centres d'intérêt ;
- etc.

PRÉVENTION ET SIGNALEMENT DES CAS DE RADICALISATION

3 Initier une démarche de signalement

Il s'agit de **prévenir, voire d'éviter, le basculement vers un comportement violent,** ainsi que d'accompagner les jeunes et les familles par des cellules adaptées au sein des préfectures de leur département de résidence.

L'objectif du signalement est de **protéger l'intéressé en l'empêchant de commettre un acte criminel** (pour le sortir au plus tôt du chemin sur lequel il s'est engagé peut-être malgré lui) et de **protéger la population** de possibles comportements violents.

Prendre l'initiative d'appeler le numéro vert constitue un simple signalement. Il appartiendra aux spécialistes d'en évaluer le caractère sérieux et la gravité.

Dans quels cas pouvez-vous appeler ?

- Pour signaler une situation inquiétante, qui paraît menacer un proche.
- Si vous avez un doute ou des questions sur une situation.
- Pour obtenir des renseignements sur la conduite à tenir.
- Pour être écouté(e), conseillé(e) dans vos démarches.

Appeler le numéro vert : **0 800 005 696**
Les appels sont strictement confidentiels, votre identité ne sera pas dévoilée.
Ou remplissez le formulaire en ligne :
https://www.interieur.gouv.fr/Dispositif-de-lutte-contre-les-filieres-djihadistes/Assistance-aux-familles-et-prevention-de-la-radicalisation-violente/Votre-signalement
Ou contacter le commissariat de police ou la brigade de gendarmerie la plus proche.
Mais en cas d'urgence appelez immédiatement le 17.

4 Que se passe-t-il après un signalement ?

Si la situation est jugée préoccupante par les services de l'État, la personne faisant l'objet du signalement ainsi que sa **famille bénéficieront d'un accompagnement spécialisé et adapté à leur situation.**

Votre identité ne sera pas dévoilée, les signalements sont strictement confidentiels. Même si vous n'êtes pas sûr d'avoir reconnu des combinaisons de signes de comportement suspect, **vous pourriez sauver des vies.** Il est donc préférable d'appeler rapidement le numéro vert. Des spécialistes se chargeront de qualifier la situation de préoccupante ou non.

Signaler une situation ne vous sera jamais reproché. Il n'est jamais trop tard pour signaler une situation de radicalisation.

5 Signaler un contenu appelant à la haine ou faisant l'apologie du terrorisme sur Internet

Internet et les média sociaux ont favorisé la diffusion d'appels à la haine et de messages faisant l'apologie du terrorisme sur la toile.

La liberté d'expression est un élément fondamental de notre société. Elle ne constitue toutefois pas un « passe-droit » pour tout rédiger et publier sur Internet. En 2009, la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation, également appelée PHAROS, a été mise en place par l'État pour signaler les comportements illicites sur Internet.

Lorsque vous constatez des contenus appelant à la haine ou faisant l'apologie du terrorisme sur Internet, ne les partagez pas, ne les likez pas, ne les retweetez pas. Ayez le bon réflexe, signalez les sur :

https://www.internet-signalement.gouv.fr

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

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

Maquette : Pôle graphique, fabrication, déploiements, image – DSAF/DPSG – Juin 2021.

Destinataires

Présidence de la République

Monsieur Laurent NUÑEZ, coordonnateur national du renseignement et de la lutte contre le terrorisme.

Premier ministre

Madame Claire LANDAIS, secrétaire générale du Gouvernement, haut fonctionnaire de défense et de sécurité.

Monsieur Denis ROBIN, secrétaire général de la mer.

Monsieur Michaël NATHAN, directeur du service d'information du Gouvernement.

Ministère de l'Europe et des affaires étrangères

Madame Hélène TREHEUX-DUCHENE, directrice générale de l'administration et de la modernisation, haut fonctionnaire correspondant de défense et de sécurité.

Ministère de la transition écologique

Ministère de la cohésion des territoires et de relations avec les collectivités territoriales

Ministère de la mer

Madame Emilie PIETTE, secrétaire générale, haut fonctionnaire de défense et de sécurité.

Ministère de l'éducation nationale, de la jeunesse et des sports

Ministère de l'enseignement supérieur, de la recherche et de l'innovation

Madame Marie-Anne LEVEQUE, secrétaire générale, haut fonctionnaire de défense et de sécurité.

Ministère de l'économie, des finances et de la relance

Ministère de la transformation et de la fonction publique

Madame Marie-Anne BARBAT-LAYANI, haut fonctionnaire de défense et de sécurité.

Ministère des armées

Général de division aérienne Fabien MANDON, chef du cabinet militaire, haut fonctionnaire correspondant de défense et de sécurité.

Ministère de l'intérieur

Monsieur Jean-Benoît ALBERTINI, secrétaire général, haut fonctionnaire de défense.

Ministère du travail, de l'emploi et de l'insertion

Ministère des solidarités et de la santé

Monsieur Étienne CHAMPION, secrétaire général, haut fonctionnaire de défense et de sécurité.

Ministère de la justice

Madame Catherine PIGNON, secrétaire générale, haute fonctionnaire de défense et de sécurité.

Ministère de la culture

Monsieur Luc ALLAIRE, secrétaire général, haut fonctionnaire de défense et de sécurité.

Ministère de l'agriculture et de l'alimentation

Madame Catherine COLLINET, haut fonctionnaire de défense et de sécurité.

Copies

Présidence de la République

Monsieur Gilles ROTTE, conseiller auprès du coordonnateur national du renseignement et de la lutte contre le terrorisme.

Premier ministre

Général de corps d'armée Benoît DURIEUX, chef du cabinet militaire.

Monsieur Franck ROBINE, conseiller pour les affaires intérieures.

Monsieur Grégory FRELY, conseiller technique sécurité intérieure.

Colonel Florence GUILLAUME, cabinet militaire - adjoint gendarmerie.

Monsieur Samuel HEUZE, haut fonctionnaire adjoint de défense et de sécurité.

Ministère de l'Europe et des affaires étrangères

Monsieur Éric GERARD, haut fonctionnaire correspondant de défense et de sécurité adjoint.

Ministère de la transition écologique

Ministère de la cohésion des territoires et de relations avec les collectivités territoriales

Ministère de la mer

Monsieur Mario PAIN, secrétariat général – chef du service de haut fonctionnaire de défense et de sécurité, haut fonctionnaire de défense et de sécurité adjoint.

Ministère de l'éducation nationale, de la jeunesse et des sports

Ministère de l'enseignement supérieur, de la recherche et de l'innovation

Monsieur Philip ALLONCLE, haut fonctionnaire adjoint de défense et de sécurité.

Ministère de l'économie, des finances et de la relance

Ministère de la transformation et de la fonction publique

Monsieur Christian DUFOUR, haut fonctionnaire de défense et de sécurité adjoint.

Ministère des armées

Colonel Rémi COTTIN, état-major des armées.

Ministère de l'intérieur

Monsieur Pierre GAUDIN, haut fonctionnaire de défense adjoint.

Monsieur Alain THIRION, directeur général de la sécurité civile et de la gestion des crises.

Monsieur Frédéric VEAUX, directeur général de la police nationale.

Général d'armée Christian RODRIGUEZ, directeur général de la gendarmerie nationale.

Monsieur Nicolas LERNER, directeur général de la sécurité intérieure.

Monsieur Pierre-Henry BRANDET, délégué à l'information et à la communication ;

Madame Laurence GOLA-DE MONCHY, sous-directrice de la protection.

Ministère du travail, de l'emploi et de l'insertion

Ministère des solidarités et de la santé

Général (2S) Arnaud MARTIN, haut fonctionnaire adjoint de défense et de sécurité, chef du pôle « protection et sécurité de défense ».

Monsieur Jérôme SALOMON, haut fonctionnaire adjoint de défense et de sécurité, chef du pôle « défense et sécurité sanitaire ».

Ministère de la justice

Colonel Éric CHUBERRE, haut fonctionnaire adjoint de défense et de sécurité

Ministère de la culture

Madame Dominique BUFFIN, haut fonctionnaire adjointe de défense et de sécurité.

Ministère de l'agriculture et de l'alimentation

Madame Hélène CALLON, haut fonctionnaire adjoint de défense et de sécurité.

<u>Diffusion interne</u> (par messagerie)

SG	M. BOUILLON
SGA	GCA DE WOILLEMONT
COORD	M. DAOOD
	M. JEZEQUEL
AIST	M. SIMON-MICHEL
	GBR WALLAERT
ANSSI	IGA POUPARD
	COL NAEGELEN
	M. VERHOEVEN
	M. BRILLANT
	M. COUTURIER
PSE	M. DE MAISTRE
	M. TREVISANI
	M. MONCONDUIT
	M. SIMON
	Mme MUNSCH
	ACAM DUCAMIN
	COL LUKIC
	CF HUET
	LCL LABEDIE
	COL BERNABE
	Mme LE NAIL
	M. DUDIT
	Mme BEAUSSANT
	M. MURGADELLA
	Dr LACHENAUD
	Mme ARNOULD