PRÉFET
DE LA MOSELLE
Liberté
Égalité
Fraternité

Cabinet
Direction des sécurités
Pôle sécurité intérieure

Metz, le 22 JUIN 2022

POSTURE VIGIPIRATE

La nouvelle posture Vigipirate « été - a*utomne 2022* » est active à compter du 22 juin 2022 et maintient l'ensemble du territoire national au niveau « ***sécurité renforcée - risque attentat*** ».

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

- la sécurité des sites touristiques et des transports publics de personnes, en particulier lors des vacances scolaires et universitaires ;
- la sécurité des espaces de commerce et des lieux de rassemblement, y compris des lieux de culte ;
- la sécurité des bâtiments publics (services publics, locaux associatifs ou politiques, écoles et universités, ainsi que les établissements de santé, sociaux et médico-sociaux) ;
- la sécurité des sites de production, de stockage et de distribution de produits de santé.

Attentions particulières dans le cadre de cette adaptation de la posture VIGIPIRATE « été - *automne 2022* » :

1 – vigilance et mesures de sécurité dans et aux abords des commissariats de police et des brigades de gendarmerie, notamment s'agissant des accueils. Les consignes aux fonctionnaires de police et aux militaires de la gendarmerie, de vigilance et d'attention à observer pour leur propre protection, dans l'exercice de leurs missions et en dehors du service sont renouvelées.

2 – maintien de l'activation des mesures prises à la suite de l'offensive des forces armées russes en Ukraine, dans le cadre de l'addendum à la posture Vigipirate « hiver 2021-printemps 2022 » qui vous a été transmis le 2 mars 2022.

3 – renforcement des mesures de sécurité du numérique des administrations et des entreprises privées au regard des menaces, avec l'application de la mesure suivantes :

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

Compte tenu des attaques menées par DdoS (une attaque par déni de service distribué -DDoS- est une arme de cybersécurité visant à perturber le fonctionnement des services ou à extorquer de l'argent aux organisations ciblées) et du risque de défiguration de sites web, il est important de s'assurer que les opérateurs de services numériques, d'une part, disposent d'infrastructures et composants de sécurité permettant d'absorber le trafic et qu'ils puissent transmettre à leurs clients une liste d'adresses IP illégitimes à bloquer et d'autre part, qu'ils assurent le renforcement des leurs systèmes d'information et des sites web hébergés.

En application du plan VIGIPIRATE l'ensemble du territoire national est maintenu au niveau « sécurité renforcée-risque attentat ».

Rappel : le logo « sécurité renforcée-risque attentat » doit être affiché à l'entrée des sites accueillant du public.

Le contexte général

La période couverte par la posture *«été – automne 2022»* est marquée par les flux importants de voyageurs dans les transports collectifs de personnes lors des vacances estivales, et l'encadrement de la sécurité sanitaire des manifestations à forte affluence ou au caractère symbolique marqué. La gestion des flux et des files doivent faire l'objet d'une vigilance accrue.

La France a informé la Commission européenne d'une nouvelle reconduction de la prolongation des contrôles aux frontières intérieures jusqu'au 31 octobre 2022 du fait d'une menace maintenue à un niveau élevé (verdict du procès du 13 novembre et situation internationale défavorable).

I. Adaptation de la posture Vigipirate « été - automne 2022 »

La posture Vigipirate « *été – automne 2022* », **maintient le territoire national au niveau « *sécurité renforcée - risque attentat* ».**

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 sollicité.
Les responsables de sites sont invités à adapter les mesures de sûreté qui leur incombent en fonction des vulnérabilités particulières des lieux, de la fréquentation et des amplitudes horaires d'ouverture (jour / nuit), du contexte local évalué avec les services de l'État sus-cités. Les personnels de l'équipe d'organisation sont 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 demeure 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 reste 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.) bénéficient de moyens adaptés. Les services de l'État (forces de sécurité

intérieure – unités Sentinelle) adaptent leur dispositif en conséquence. Les opérateurs sont 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.

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 demeure renforcée autour des grands espaces de rassemblements ayant pour objet des activités commerciales (salons d'expositions, foires, etc.) en particulier lors des soldes d'été, marquées par une forte affluence. Les interconnexions de transports en milieu clos dotées de commerces (métros, gares, etc.) demeurent également un point de vigilance.

Une vigilance accrue est maintenue notamment sur le secteur du tourisme et des parcs de loisirs, particulièrement fréquentés au moment des vacances scolaires.

Lorsque des éléments objectifs attestent d'une menace sur le plan local, ou qu'un événement révèle une vulnérabilité particulière, ceux-ci sont communiqués par l'autorité préfectorale 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 réguliers 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 sera accordé aux espaces de commerce, dans toute la mesure du possible, l'extension de leur vidéosurveillance aux abords immédiats sur la voie publique (seules la police nationale et la gendarmerie peuvent visionner les images captées sur la voie publique – Cf. article L.252-2 du code de la sécurité intérieure). Par ailleurs, pour les espaces complexes le justifiant, le recours à la notion de « périmètre vidéoprotégé » peut-être utilement envisagé.

De même, seront examinées 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.

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.

➢ *Objectifs de sécurité recherchés sur la période*

- *Espaces d'accueil des voyageurs pour tout mode de transport*

La menace visant les emprises des gares ferroviaires ou routières et celle de l'aéroport de Metz-Nancy-Lorraine, notamment, impose la poursite d'une vigilance attentive.

- *Spécificité du transport aérien*

Les gestionnaires d'aéroports et les compagnies aériennes doivent maintenir leur haut niveau de vigilance lors des contrôles d'embarquement des passagers. Les services de l'Etat et les opérateurs poursuivent l'amélioration de la sécurisation du côté ville.

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 et de la cohésion des territoires par SNCF Réseau :

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

4 - Sécurité des bâtiments publics

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

Un effort particulier est porté sur la protection de la préfecture, des sous-préfectures et de l'ensembre des sites préfectoraux et/ou interministériels.

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

Les annuaires de crise doivent être actualisés 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 doivent être portés à la connaissance des nouveaux arrivants.

Une vigilance particulière est également portée à la sécurité des palais de justice et des établissements pénitentiaires dans le contexte de procès dits « sensibles ».

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

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 2021-2022, la passation des examens, 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 2022-2023 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 prennent 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. La complémentarité des actions au sein de l'appareil de gestion de crise décliné à l'échelon territorial est fondamentale, et doit être systématiquement recherchée.

➢ *Objectifs de sécurité recherchés sur la période*

- Reconduction des principales mesures Vigipirate : surveillance des emprises et leurs abords contrôle des accès.

- Sécurisation des personnes et des biens au moyen des plans de sécurisation et des exercices

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 les établissements scolaires.** Le déploiement des diagnostics de mise en sûreté doit se poursuivre.

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.

Dans les établissements et les sites des opérateurs sous tutelle des MENJS/MESRI et du ministère de l'agriculture et de l'alimentation (MAA), une attention particulière est 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 procédures 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 à :

- la sensibilisation régulière des apprenants et des personnels aux menaces cyber et aux bonnes pratiques à adopter au quotidien, en particulier sur les menaces relatives au hameçonnage (phishing),
- la protection à un niveau adéquat des locaux dédiés à l'hébergement des systèmes d'information, des stockages de données et des systèmes de restauration, en s'assurant également de la capacité à disposer de sauvegardes déconnectées ou résistantes aux rançongiciels,
- la mise en œuvre d'une politique de campagnes récurrentes de renouvellement des mots de passe de tous les usagers en prenant en compte les nouveaux standards,
- la mise en œuvre d'une politique active des mises à jour de sécurité des applications et infrastructures numériques,
- la remontée systématique d'incidents de sécurité numérique auprès du responsable de la sécurité des systèmes d'information du périmètre concerné.

6 - Sécurisation des sites touristiques, culturels et des expositions à thème sensible

Le retour des touristes et la disparition des contraintes liées aux jauges sanitaires renforcent le risque de formation de files d'attente à l'entrée des établissements et événements culturels. Le ministère de la Culture recommande par conséquent l'application des mesures de prévention répertoriées dans les guides pratiques disponible en ligne : http://www.culture.gouv.fr/Actions-de-renforcement-et-de-surveillance-des-lieux-culturels.

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.

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).

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 solidaritées et de la santé.

Point d'attention :

- les opérateurs d'importance vitale continuent de 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*

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, 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.

8 - 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 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 aux responsables de la sécurité des systèmes d'informations 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 31-03 – Absorber le trafic illégitime au niveau du réseau :

- Compte tenu des attaques menées par DDoS et du risque de défiguration de sites web, il est important de s'assurer que les opérateurs de services numériques, d'une part, disposent d'infrastructures et composants de sécurité permettant d'absorber le trafic et qu'ils puissent transmettre à leurs clients une liste d'adresses IP illégitimes à bloquer et d'autre part, qu'ils assurent le renforcement des leurs systèmes d'information et des sites web hébergés.

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 centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (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 effectuée.

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 est familiarisé avec celui-ci. Il est par ailleurs recommandé d'effectuer un exercice d'activation du plan de continuité d'activité (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/

II. Consignes particulières de vigilance, prévention et protection

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 sont sensibilisées et informées par leurs autorités de tutelle des mesures de sécurité à appliquer.

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

Les attaques par véhicules-béliers demeurent un mode d'action 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 ;

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).

4 - 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 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.

III. Sensibilisation des professionnels et du grand public

Le niveau élevé de la menace exige le maintien d'une vigilance accrue.

Maintien des logogrammes

Ils peuvent être téléchargés sur les sites :

http://www.gouvernement.fr/vigipirate ;

http://www.sgdsn.gouv.fr/vigipirate .

Dans un souci de large diffusion des bonnes pratiques face à la menace terroriste, des fiches renouvelées de sensibilisation à destination, tant du grand public que des professionnels 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) a diffusé 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 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.

Vous trouverez en annexe :

- Drones : règles d'utilisation et mesures de prévention face à un usage malveillant

Le préfet,

Laurent Touvet

VIGIPIRATE

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.
Son utilisation est soumise à des règles, et la prévention des actes malveillants nécessite quelques bonnes pratiques.

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 autorisation 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 ;
- **enregistrer** le drone si celui-ci a une masse supérieure à 800 grammes ;
- **me conformer** à l'obligation de signalement électronique si le drone a une masse supérieure à 800 grammes ;
- **respecter les zones interdites** de survol en consultant le site Géoportail de l'IGN ;
- **respecter la vie privée d'autrui ;**
- **souscrire** un contrat d'assurance prenant en compte mon activité ;
- **respecter la réglementation** en matière d'interdiction de prise de vue aérienne (arrêté du 27 octobre 2017).
- **Consulter le site de la DGAC** pour prendre connaissance de la réglementation en vigueur, et retrouver tous les liens vers les sites utiles :

https://www.ecologie.gouv.fr/exploitation-drones-en-categorie-ouverte#scroll-nav__1

** Cadre des usages de loisirs et professionnels simplifiés, dit « catégorie ouverte ». Le recours à un exploitant professionnel de drones offre un cadre d'emploi plus large dit « catégorie spécifique » qui peut être mieux adapté à certains besoins. (https://www.ecologie.gouv.fr/exploitation-drones-en-categorie-specifique)*

VIGIPIRATE

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 manifestation que j'organise, je dois :

- **inclure** la menace-drone dans mon plan de sécurité et de secours ;
- **me rapprocher** des services de la préfecture afin de consulter les éventuelles déclarations ou autorisations d'activité drone aux abords de la manifestation et d'identifier les potentielles mesures de prévention à mettre en œuvre ;
- **étudier** la mise en place de moyens de détection de drones ;
- **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, image – DSAF/DPSG – Mai 2022.