PRÉFET
DE LA LOIRE-
ATLANTIQUE
Liberté
Égalité
Fraternité

CABINET DU PRÉFET
Service interministériel régional
des affaires civiles et économiques
de défense et de la protection civile

Affaire suivie par :
pref-defense-protection-civile@loire-atlantique.gouv.fr

Nantes, le 19 juin 2023

Le Préfet de la région Pays de la Loire,
Préfet de la Loire-Atlantique

à

Destinataire *in fine*

Objet : Adaptation de la posture VIGIPIRATE « été - automne 2023 »

La nouvelle posture VIGIPIRATE pour la période « été-automne 2023 » sera activée à compter du mercredi 21 juin 2023 et maintiendra l'ensemble du territoire national au niveau de « **sécurité renforcée — risque attentat** ». Des mises à jour pourront être diffusées en fonction du contexte et de l'évolution de la menace.

Elle permet d'adapter le dispositif en prenant en compte la période estivale et ses flux importants de voyageurs dans les transports collectifs. Elle voit l'activation de mesures spéciales uniquement pour la période du 1er septembre au 1er novembre dans les zones concernées par l'accueil de matchs de la Coupe du monde de rugby – France 2023.

En outre, la posture VIGIPIRATE « été-automne 2023 » adapte le dispositif et met l'accent sur :

- La sécurité des sites touristiques et des transports publics de personnes ;
- 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).

Plusieurs axes d'effort s'appliquent en matière de vigilance, de prévention et de protection. Ils tiennent compte de l'analyse de la menace et des vulnérabilités de la période considérée.

1 – Adaptation de la posture Vigipirate « été-automne 2023 »

1.1 – Sécurité de la coupe du monde de rugby 2023

Elle se déroulera du vendredi 8 septembre au samedi 28 octobre, en réunissant 20 équipes pour 48 matchs. A Nantes, ville hôte, les 4 matchs auront lieu les 16 (Irlande-Tonga) et 30 (Argentine-Chili) septembre et les 7 (Pays de Galle-Géorgie) et 8 (Argentine-Japon) octobre. Un village rugby sera ouvert. La ville de la Baule sera le camp de base de l'équipe d'Argentine.

Cet événement sera une vitrine médiatique internationale et un vecteur de concentration de foules, il pourra être une cible privilégiée pour tous types d'individus ou groupes malveillants.

Plusieurs directives sont matérialisées via des instructions ministérielles envoyées aux Préfets de département et traitées dans les groupes de travail mis en place depuis juillet 2022.

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

1.2.1 – 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 évènement, les responsables et initiateurs doivent impérativement prendre contact avec les forces de sécurité intérieure (FSI) et les services préfectoraux quand bien même l'avis des référents sûreté départementaux de la police ou de la gendarmerie a été sollicité.
Les responsables de sites sont invités à adapter les mesures de sûreté qui leur incombent en fonction des vulnérabilités particulières des lieux, de la fréquentation et des amplitudes horaires d'ouverture (jour/nuit), du contexte local évalué avec les services de l'État.

Les personnels de l'équipe d'organisation seront sensibilisés aux bons comportements à adopter en cas de situation suspecte, de menace d'attaque terroriste, de confinement ou d'évacuation selon les situations.

1.2.2 – Objectif de sécurité recherché sur la période

- **Mesures propres aux fêtes religieuses se déroulant tout au long de l'année**

Quel que soit le culte concerné (mais plus particulièrement les cultes chrétien, juif et musulman), la sécurité devra être renforcée autour des lieux de culte avec un effort sur la présence visible des forces de l'ordre ou des militaires de l'opération Sentinelle selon un mode de sécurisation dynamique, assorti de prise de contact avec les responsables des lieux.

En liaison avec les autorités religieuses locales, il est recommandé de prévoir des mesures de contrôle des accès (limitation du nombre d'accès, contrôle visuel des flux...). Une vigilance particulière doit être portée sur les véhicules de stationnement à proximité des lieux de culte. À cet effet, les maires pourront prendre des mesures temporaires d'interdiction de circuler et de stationner autour de ces lieux de culte.

- **Mesures propres aux périodes de vacances scolaires**

Les lieux sujets à de fortes affluences saisonnières durant les vacances scolaires (ex : salles de spectacles...) 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 évènement de voie publique**

Le ministère de l'Intérieur a publié et diffusé un Guide des bonnes pratiques de sécurisation d'un évènement 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.

1.3 – Sécurité des grands espaces de commerce, de tourisme et de loisirs

1.3.1 – Contexte général

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

La sécurité doit rester renforcée autour des grands espaces de rassemblement ayant pour objet des activités commerciales (salon d'exposition, foires, etc) et les interconnexions de transports en milieu clos dotées de commerces (métros, gares, etc.) demeureront également un point de vigilance.

Le secteur du tourisme, les stations balnéaires et les parcs de loisirs, particulièrement fréquentés au moment des vacances scolaires, pourraient être ciblés. Par ailleurs une attention particulière doit être portée à la sécurité des grands espaces de commerce lors des soldes d'été.

De façon plus générale, il revient aux autorités préfectorales d'évaluer le niveau de sécurité à atteindre pour les différentes activités sises dans leur département. Lorsque des éléments objectifs attestent d'une menace sur le plan local, ou qu'un évènement révèle une vulnérabilité particulière, ceux-ci sont communiqués aux responsables de sûreté des établissements concernés afin de leur permettre d'adapter leur dispositif.

1.3.2 – Objectif de sécurité recherché 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'État 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'information. Le développement de ces conventions locales doit être 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, elle 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).

Le préfet examine les demandes des espaces de commerce d'autoriser, à titre exceptionnel, la présence d'agents privés de sécurité, même itinérante, sur la voie publique, aux abords de leurs sites.

1. 4 - Sécurité des transports collectifs

1.4.1 – 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, évènements sportifs ou festifs, etc.). À ces occasions, le niveau de sécurité des plateformes aéroportuaires, des gares, des ports et des réseaux de transport en commun doit être renforcé[1].

1.4.1 – Objectifs de sécurité recherché sur la période

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

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

- **Spécificité du transport aérien**

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

1 L'efficacité des mesures de contrôle dans les transports peut être accrue par le rappel des dispositions tirées des lois Savary-Darmanin, Urvoas et Leroy de 2016

➢ **Infrastructures et réseaux ferroviaires**

Les transports terrestres constituent toujours une cible d'intérêt, à la symbolique et l'impact fort. En outre, la reprise du trafic depuis plusieurs mois fait du secteur des transports une cible d'opportunité.

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.

1.5 – Transport maritime de passagers

Conformément à l'arrêté du 16 juillet 2018, les exploitants portuaires et armateurs doivent assurer la continuité du contrôle des véhicules, de leurs passagers et de leur chargement. Tout armateur exploitant des navires rouliers à passagers mettra en place un dispositif destiné à prévenir l'introduction d'articles prohibés par les personnes en sortie des espaces rouliers, au moment de leur accès aux espaces publics du navire. A ce titre, les efforts de criblage, qui reposent sur l'analyse et la détection de comportements particuliers avant l'embarquement, en liaison avec les autorités portuaires sont reconduits.

1. 6 – Sécurité des bâtiments publics

1.6.1 – 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.

Il convient d'actualiser les annuaires de crise 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 dédiée 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 fait de terrorisme. La sécurisation des juridictions abritant ces occurrences constituera un axe d'effort spécifique.

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 ; et les **services pénitentiaires d'insertion et de probation** préparant l'insertion ou la réinsertion des personnes placées sous main de justice confiées dont certaines sont radicalisées et/ou condamnées pour terrorisme (participation à des actions violentes ou à une association terroriste) et à assurer le suivi des mesures et peines exécutées en milieu libre, en collaboration avec des partenaires publics et associatifs.

1.7 – Sécurisation des établissements d'enseignement et de recherche, des établissements publics du ministère chargé des sports et des structures d'accueil collectif de mineurs (ACM) à caractère éducatif, ainsi que des structures d'accueil des séjours de cohésion du SNU des établissements publics relevant du ministère des sports et des jeux olympiques et paralympiques.

L'adaptation de cette posture maintient les mesures antérieures et met l'accent sur :

- L'organisation ministérielle et les liens entre services de l'État dans le cadre de la coupe du monde de rugby ;
- Le travail partenarial avec les acteurs concourant à la préparation des jeux olympiques et paralympiques 2024 ;
- Les mesures de sécurisation nécessaires à prendre en lien avec les préfectures de départements, les collectivités territoriales et les opérateurs, face aux risques d'intrusion ou de toute atteinte à la sûreté d'un établissement ;
- La mise à jour des plans particuliers de mise en sûreté (ou document assimilé) et des plans de continuité d'activité (PCA). Prévoir la réalisation d'exercices associés. En cas d'évènement perturbant le fonctionnement de l'établissement concerné, le responsable du site doit prendre toute mesure nécessaire (activation du PPMS, du PCA, de son dispositif de crise ...) et en informer les autorités compétentes ;

- Le signalement aux forces de sécurité intérieure de toute menace proférée à l'encontre des personnels exerçant une mission de service public ou lors de diffusions relatives à sa vie privée, familiale ou professionnelle[2] ;
- Le séjour de cohésion dans le cadre du service national universel ;
- Le maintien d'une haute vigilance à la sécurisation des systèmes d'information

1.7.1 – Contexte général

Les établissements d'enseignement et de recherche sont des cibles privilégiées, quelle que soit l'origine de la menace, en raison notamment de leur charge symbolique.

Les mesures des directives ministérielles et interministérielles doivent être mises en œuvre au sein des établissements et organismes relevant des ministères avec les préfectures, les forces de sécurité intérieure, les collectivités territoriales et les responsables de structures privées accueillant le public des MENJ/MESR/MSJOP.

1.7.2 – Objectifs de sécurité recherchés sur la période

➢ **Coupe du monde de rugby 2023**

L'enjeu sécuritaire et médiatique de la coupe du monde de rugby appelle également une organisation adaptée du MSJOP. Une haute vigilance des impacts des grands évènements sportifs sur le périmètre MSJOP devra être assurée. Les régions académiques et établissement du MSJOP mettront en œuvre les mesures des directives interministérielles.

Il importe également que des liens renforcés soient déployés entre les services de l'État et les collectivités territoriales hôtes, dans un souci de partage d'informations et de gestion d'incidents ou d'évènements graves le cas échéant.

➢ **Sécurisation des personnes et des biens**

- Maintien des consignes en vigueur

Les établissements et les organismes du MENJ/MESR/MASA doivent maintenir leurs efforts de sécurisation des personnes et des biens (personnels et usagers), par exemple :

- ✔ L'élaboration et/ou la mise à jour des diagnostics de sûreté et des plans particuliers de mise en sûreté (PPMS) ;
- ✔ Le contrôle des flux de personnes, des marchandises et des véhicules ;
- ✔ Le contrôle des sacs à l'entrée des établissements à chaque fois que cela est possible ;
- ✔ La surveillance active aux abords des établissements ;
- ✔ L'élaboration et/ou la mise à jour des dispositifs de gestion de crise ;
- ✔ La formation et la sensibilisation des personnels aux enjeux de sûreté ;
- ✔ Un contrôle des accès aux différents sites et emprises bâtimentaires.

- Maintien d'une vigilance particulière des sites sensibles

Dans les établissements et les sites des opérateurs sous tutelle des MENJ/MESR et du MASA, une attention particulière sera portée à la protection et aux contrôles des laboratoires sensibles soumis à une réglementation spécifique, ainsi qu'aux lieux de stockage des matières dangereuses ou abritant des animaleries.

Les zones considérées comme sensibles doivent faire l'objet d'une vigilance maximale, de procédure de contrôle renforcé et de signalements systématiques.

Dans le périmètre du MESR et du MASA, dans tous les cas, y compris hors cas prévus par les dispositions réglementaires encadrant le dispositif de protection du potentiel scientifique et technique, le fonctionnaire de sécurité de défense/ officier de sécurité (OS) de l'établissement doit être informé de toute problématique sécuritaire et en faire part au HFDS du périmètre ministériel dont relève son établissement.

- Sécurisation des systèmes d'information (données et infrastructures numériques)

Il est demandé aux services et établissements des MENJ/MESR de veiller aux consignes relayées par le fonctionnaire de sécurité des systèmes d'information.

2 Conformément aux consignes adressées aux recteurs dans la circulaire du 9 novembre 2022 relative au plan pour la laïcité dans les écoles et les établissements scolaires.

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

Vu le contexte international et la persistance d'un niveau élevé de menace, les exploitants de sites touristiques sont invités à renforcer leurs mesures de vigilance et à prendre l'attache des forces de sécurité intérieure.

Les organisateurs des événements se déroulant sur la voie publique, plus nombreux en période estivale, sont invités à se référer au guide des bonnes pratiques de sécurisation d'un événement de voie publique disponible sur le site internet du ministère de l'Intérieur[3].
L'attention des propriétaires de monuments désirant participer aux 40ème Journées du patrimoine est tout particulièrement attirée sur les mesures de précaution élémentaires et la nécessité de manifester auprès du commissariat ou brigade la plus proche cet événement. Les éléments de vigilance accrue concernent également les sites à forte valeur symbolique du point de vue historique et exploités annuellement.

À l'approche des Jeux Olympiques et Paralympiques de Paris qui se déroulent sur l'ensemble du territoire national, une série d'évènements culturels labellisés auront lieu sur vos territoires. Ces évènements en plus de la valeur symbolique inhérente aux sites retenus peuvent s'avérer particulièrement exposés à la menace terroriste du fait de leur association au mouvement olympique.
Les acteurs culturels sont invités à appliquer les mesures de prévention répertoriées dans les guides pratiques disponibles en ligne[4]. Ils devront prendre attache des forces de sécurité intérieure (police nationale et gendarmerie nationale).

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.

1.9 – Sécurité des opérateurs relevant des ministères sociaux

Ces opérateurs (santé, solidarité, travail) demeurent des cibles vulnérables. Plusieurs thématiques et projets de réforme sensible (votés ou non) pourraient amener des individus à commettre des actes de nature terroriste. Il convient donc d'avoir une vigilance élevée de la part des opérateurs pré-cités.

1.9.1 – Secteurs santé et solidarités

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, sociaux et médico-sociaux poursuivent le déploiement de leur stratégie de protection, en suivant les recommandations du ministère de tutelle. 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) d'autant plus à l'approche de la préparation des grands événements sportifs internationaux se déroulant en France. Les établissements à proximité des sites sportifs où se dérouleront ces événements veilleront à vérifier, mettre à jour voire renforcer en tant que de besoin leur dispositif de sécurisation.

Point d'attention :

- les opérateurs d'importance vitale (vigilance toute particulière dans la continuité de la crise sanitaire actuelle) ;
- établissements de santé accueillant des mineurs dans le cadre du bilan somatique et médicopsychologique (conformément aux termes de l'instruction du 23 février 2018 relative à la prise en charge des mineurs de retour de zone d'opérations de groupements terroristes, notamment la zone irako-syrienne) ;
- les systèmes d'information : ils sont les cibles d'attaques du fait de leurs vulnérabilités. Le risque est majoré par un état de la menace cyber préoccupant.

1.9.2 – Secteur travail

3 https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenments-de-voie-publique
4 http://www.culture.gouv.fr/Actions-de-renforcement-et-de-surveillance-des-lieux-culturels

Les agences et opérateurs chargés de la mise en œuvre locale des politiques de l'emploi peuvent constituer des cibles symboliques pour des individus souhaitant attaquer l'État. Ils veilleront, dans un probable contexte où des individus pourraient profiter de la vitrine d'un des événements internationaux pour porter leurs revendications par des contestations éventuellement violente, à demeurer en contact avec les FSI locales en cas de tensions et de contestations violentes.

1.10 – Sécurité du numérique (ANSSI)

1.10.1 – Contexte général

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

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

1.10.2 – Objectifs de sécurité recherchés sur la période

Au regard de l'évaluation de la menace pour la sécurité du numérique présentée ci-dessus, il apparaît nécessaire d'appliquer les objectifs et mesures de sécurité suivants :

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

Compte tenu de l'évolution de la menace, il est recommandé de :

- ✔ Mettre en place un processus pour consulter régulièrement les rapports de la menace sur le site du CERT
- ✔ Récupérer les marqueurs associés et les relayer à l'ANSSI

Ces marqueurs peuvent être intégrés aux systèmes de détection disponibles (antivirus, EDR, NDIS, HIDS,...). Par ailleurs, il est recommandé de chercher la présence de ces derniers sur l'historique des journaux disponibles afin d'identifier d'éventuelles tentatives de compromission.

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

Afin de prémunir d'éventuelles attaques suite à la découverte de vulnérabilités, il convient de mettre en place un processus de veille concernant la publication de vulnérabilités relatives aux éléments du DI. Il est possible de s'appuyer sur les bulletins du CERT-FR. Cette veille doit être réalisée de manière quotidienne, idéalement via un processus automatisé à partir de sources complémentaires pour couvrir l'ensemble des briques du SI.

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

Compte tenu des attaques menées 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 de leurs systèmes d'information et des sites web hébergés.
Il est nécessaire d'identifier les moyens de filtrage les plus efficaces. Il est recommandé de prendre en compte les différentes typologies d'attaques par déni de service et la couverture offerte par les moyens de filtrage. Les organisations doivent ensuite mettre en place ces mécanismes de protection anti-déni de service sur les services qu'ils hébergent ou demander la mise en place auprès des prestataires d'hébergement ou de communication le cas échéant.

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

Il convient de sensibiliser régulièrement les utilisateurs aux risques numériques et à l'application de la politique de sécurité des SI, en particulier vis-à-vis de l'utilisation de support amovibles, de navigation internet ou d'échange de courriels.
La non-séparation des usages et matériaux personnels et professionnels, échanges professionnels dans les lieux publics, présence de matériaux protégés ou classifiés sur des systèmes inadéquats sont à proscrire.

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

Face aux vulnérabilités critiques et à l'état de la menace, il est impératif d'appliquer, dans les plus brefs délais, les correctifs de sécurité mentionnés dans les bulletins d'alerte de sécurité du CERT-FR. Les correctifs référencés dans les alertes doivent, si cela est nécessaire et pour des raisons d'urgence et de

criticité, être appliqués en dehors des processus de maintien en condition de sécurité des SI. Ils doivent également être appliqués dans le cycle habituel de maintien en condition de sécurité des SI. L'exploitation de certaines des vulnérabilités référencées permet l'accès à des comptes privilégiés pour l'attaquant et étend ses capacités de latéralisation sur les systèmes. La bonne application des correctifs de sécurité référencés doit être régulièrement contrôlée et validée. Les bulletins d'alerte de sécurité et les avis de sécurité sont disponibles sur le site du CERT-FR.

- **Vérifier les annuaires de crise et le fonctionnement des moyens de communication sécurisés**

Face aux menaces, il convient de s'assurer que la capacité de communication entre les personnels en charge de répondre à la crise sera maintenue. Il est essentiel de vérifier les contacts internes et externes des annuaires de crise. Par ailleurs, certaines menaces pouvant aboutir à la perte des outils de communication usuels, il est nécessaire de tester régulièrement les moyens de communication alternatifs et sécurisés utilisés dans le cas d'une attaque impactant les outils de communication nominaux.

- **Procéder régulièrement à un séquestre hors ligne exceptionnelle des sauvegardes des systèmes les plus critiques**

En cas d'attaque par rançongiciel, 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[5].

2 – Consignes particulières de vigilance, prévention et protection

2.1 – 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.

2.2 – 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'évènements 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 ci-avant.

2.3 – Signalements des cas suspects de radicalisation, des troubles comportementaux ou psychiatriques/psychologiques

La radicalisation se caractérise par un changement de comportement qui peut conduire certaines personnes à l'extrémisme ou au terrorisme. Des troubles psychologiques peuvent favoriser la radicalisation. Il est important de signaler ces personnes au Centre National d'Assistance et de Prévention de la Radicalisation (CNAPR) afin de protéger ces personnes d'elles-mêmes et contre de possibles comportements violents envers la population. Ces situations doivent alerter et méritent de faire l'objet d'un signalement :

- Changements physiques, vestimentaires et alimentaires ;
- Propos asociaux ;
- Passage à une pratique religieuse hyper ritualisée ;
- Rejet de l'autorité ;
- Repli sur soi ;
- Rejet brutal des habitudes quotidiennes ;
- Refus du débat ;
- Rejet de la société et des institutions ;
- Modification soudaine des centres d'intérêt
- Discours complotistes ou apocalyptiques
- Tentative d'imposition agressive d'un ordre religieux

5 https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf

Le signalement des cas suspects de radicalisation se réaliser au numéro vers suivtant : **0 800 005 696**. En cas de suspicion d'une action violente ou de tout autre cas d'urgence, appeler immédiatement le 17 ou le 112 pour alerter les forces de sécurité intérieure.

2.4 – 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. Ce point de vigilance a justifié l'envoi d'un bulletin flash le 12 décembre 2022.

Au moindre doute sur le contenu d'un colis ou d'une enveloppe, ce dernier ne doit pas être manipulé. Il doit être contrôlé au moyen d'un détecteur à rayon X. En cas d'impossibilité à mettre en œuvre ce type de technologie, il convient d'alerter les forces de sécurité intérieure en réalisant un appel au 17 et d'établir un périmètre de sécurité en faisant évacuer et en balisant la zone.

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).

Conformément à la circulaire n° 750/SGDSN/PSE/PPS du 18 février 2011, la découverte de plis, colis ou contenants et substances suspectés de renfermer des agents NRBC dangereux relève de la gestion d'un trouble à l'ordre public quel que soit le traitement de cette découverte (administratif, judiciaire, sanitaire, etc.). La pertinence des premières mesures prises par les services de police ou de gendarmerie, sous l'autorité du représentant de l'État dans le département, après contact avec la cellule nationale de conseil (01 49 27 49 27 – H24/365 jours par an), vise à éviter une mobilisation de moyens disproportionnée par rapport au risque. La cellule nationale de conseil a pour missions de recueillir et d'analyser les premiers éléments de l'enquête, d'assurer le conseil auprès des autorités requérantes et d'informer les Hautes autorités en charge de la préparation et de la réponse de l'État face à un évènement terroriste NRBC.

2.5 – 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, mais qui peut évoluer vers des actes de malveillance ou terroristes. Les responsables d'activités sensibles et de grands rassemblements doivent prendre en compte cette menace en sollicitant l'avis des référents sûreté locaux de la police ou de la gendarmerie nationale, ayant la possibilité de mettre en œuvre des moyens de détection.

Les évènements les plus sensibles peuvent également donner lieu, en fonction de l'évaluation de la menace et sur décision de la Première ministre, au déploiement d'un dispositif particulier de sûreté aérienne (DPSA) placé sous le commandement du commandant de la défense aérienne et des opérations aériennes (CDAOA) et incluant des moyens de lutte anti-drone.

3 – Sensibilisation du grand public

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

3.1 – Efforts de communication

Les ministères veilleront 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 SGDSN[6].

3.2 – 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

6 https://www.sgdsn.gouv.fr/vigipirate/le-plan-vigipirate-faire-face-ensemble

renouvelées sont accessibles en ligne depuis l'espace Vigipirate du site Internet du SGDSN[7] et traitent des sujets suivants ; que faire en cas d'exposition à un gaz toxique ? Réagir en cas d'attaque terroriste ?

La communication des mesures et des comportements à adopter en cas d'attaque terroriste au sein des établissements et lieux recevant du public est fondamentale. Les affiches, qui peuvent être téléchargées et imprimées 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.).

Par ailleurs, un ensemble de fiches de recommandations et de bonnes pratiques à l'attention du grand public est également téléchargeable sur le site du SGDSN[8].

Par ailleurs, un ensemble de guides de bonnes pratiques, à destination des **élus et des professionnels** est mis à disposition sur le site du SGDSN[9]. 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 pédagogique de sensibilisation VIGIPIRATE : www.vigipirate.gouv.fr. 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.

Mes services restent à votre disposition pour tout renseignement complémentaire.

Le Préfet,

Fabrice RIGOULET-ROZE

DESTINATAIRES :

Madame la présidente du conseil régional des Pays de Loire

Monsieur le président du conseil départemental de la Loire-Atlantique

Mesdames et messieurs les maires du département de la Loire-Atlantique

Mesdames et messieurs les présidents des établissements publics de coopération intercommunale à fiscalité propre

7 https://www.sgdsn.gouv.fr/vigipirate/les-affiches-de-sensibilisation
8 https://www.sgdsn.gouv.fr/vigipirate/les-fiches-de-recommandation-et-de-bonnes-pratiques
9 https://www.sgdsn.gouv.fr/vigipirate/les-guides