PRÉFET
DE LA MOSELLE
Liberté
Égalité
Fraternité

Cabinet
Direction des sécurités
Pôle sécurité intérieure

Metz, le 16 JUIL. 2021

POSTURE VIGIPIRATE

La nouvelle posture Vigipirate « été - a*utomne 2021* » est active et maintient l'ensemble du territoire national au niveau « ***sécurité renforcée - risque attentat*** ».

Dans le contexte de crise sanitaire généré 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 des 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, médicaux-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.

Quelques changements notables sont apportés par cette nouvelle posture sur le plan de la sécurité des systèmes d'informations. Il s'agit de :

1 - la cyber sécurité des structures de santé, car le ministère des solidarités et de la santé a pris de nouvelles mesures, en coordination avec l'ANSSI, dans le cadre du « Plan de renforcement de la cybersécurité des établissements de santé » dont les 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.

Les établissements de santé principalement concernés sont les 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, ainsi que ceux qui constituent la chaîne vaccinale contre la COVID-19.

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

- mesure « NUM 11-02 » - rechercher sur le SI des marqueurs particuliers correspondant à une attaque. 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 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).

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.

I. Contexte général

1- Principaux événements sur le territoire national

La période couverte par la posture « été-a*utomne 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 évènements estivaux et la période touristique ;
- les modalités de gestion de la crise du COVID 19.

2. Prolongation des contrôles aux frontières intérieures

La France a rétabli les contrôles aux frontières intérieures le 13 novembre 2015, il a depuis été régulièrement reconduit sur le fondement de l'article 25 du code frontières.

3 Évolution du contexte juridique (fin 2020-début 2021)

- la loi du 24 décembre 2020 relative à la prorogation des chapitres VI à X du titre II du livre II de l'article L .851-3 du code de la sécurité intérieure qui prolonge jusqu'au 31 juillet 2021 différentes mesures de lutte contre le terrorisme (fermeture administrative des lieux de culte, mesures de surveillances). La technique de renseignement dite « algorithme » est prolongée jusqu'au 31 décembre 2021. La loi prolonge par ailleurs 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.

- la loi du 26 mai 2021 pour une sécurité globale préservant les libertés qui élargit notamment aux actes de terrorisme les missions, mêmes itinérantes, de surveillance que les agents privés de sécurité sont autorisés, par le préfet, 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).

- le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement qui vise à pérenniser certaines mesures inspirées de l'état d'urgence (fermeture administrative des lieux de culte, mesures de surveillances, les « visites et saisies »). Il prévoit également de renforcer la base légale du brouillage des drones malveillants.

- 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.

- le 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.

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

II. Évaluation de la menace terroriste

Sept attaques terroristes abouties sur le territoire national en 2020 et 2021 ont fait 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 subies :

- une cristallisation des divers courants islamistes sur la question du blasphème, avec un passage à l'acte lié de façon plus ou moins affirmée à ce sujet.
- les prémices d'un phénomène d'autonomisation de la menace à la fois opérationnelle et idéologique, sans affiliation précise à un groupe terroriste et une radicalisation facilitée par des déséquilibres psychologiques ou pathologies mentales.
- un niveau de menace terroriste en prison préoccupant avec un niveau élevé de détenus de droit commun radicalisés.

Si une attaque peut être conduite en tout lieu du territoire, les principales catégories de cibles susceptibles d'être visées sont :

- **les grands rassemblements festifs** (fêtes nationales, célébrations religieuses, manifestations sportives et culturelles) ;
- **les sites symboliques** (sites touristiques, institutions publiques, bureaux de votes, sites religieux, etc.) ;
- **les lieux publics très fréquentés** (transports urbains, aéroports, gares, lieux de divertissement, établissements commerciaux) ;
- **les établissements et personnels situés au cœur du fonctionnement de notre société** (écoles, universités, hôpitaux, les centres de tests ou de vaccination, etc.) ;
- **les représentants en uniforme de l'autorité publique** (policiers, gendarmes, douaniers, militaires), tout comme les lieux où ils résident (casernes, brigades, cantonnements, etc.). Compte-tenu de la concentration de détenus radicalisés en milieu carcéral, **les personnels pénitentiaires** sont également particulièrement concernés.

III. La Cyber menace

1 - Impacts de la crise sanitaire et retour sur le lieu de travail

À la suite du déclenchement de la pandémie de COVID-19, le recours intensif au télétravail et aux outils numériques a rendu plus vulnérables les utilisateurs connectés à distance au système d'information de leur organisation car isolés de leur environnement professionnel. Il a également entraîné une augmentation de la surface d'attaque par la mise en service de nouveaux moyens de connexion à distance aux systèmes d'information en urgence ce qui a conduit parfois à une insuffisance de la prise en compte de la sécurité. Ainsi, des attaques par hameçonnage (courriels avec lien ou pièce jointe malveillante) ont été menées à des fins de captation de données ou de chantage par rançongiciel.

Le retour au travail en présentiel ainsi que le retour de congés, constituent également des périodes particulièrement critiques et propices aux attaques informatiques. Les attaquants exploitent régulièrement la baisse de vigilance des utilisateurs associée au traitement et à l'échange important de courriels (offres promotionnelles, *etc.*).

De plus, lors de ces périodes, 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 l'absence des équipes de sécurité informatique.

2 - Tendances actuelles et vulnérabilités critiques

Attaques par rançongiciel

Depuis 2020, les attaques par rançongiciel, menées par des groupes cybercriminels, ont fortement augmenté et de manière plus ciblée. Elles touchent autant des organisations publiques (ex : collectivités locales et établissements de santé) que des entreprises privées (énergie, BTP, technologies, aéronautique).

De plus, l'épidémie du COVID-19 a donné lieu à une recrudescence de ces attaques notamment par le biais de courriels sur ce thème proposant des liens ou des pièces jointes malveillantes.

Ce dernier constat est renforcé par la prolifération de rançongiciels accessibles aux cybercriminels disposant de faibles compétences techniques, d'une part, et le faible niveau de sécurité des systèmes d'information des entités victimes, d'autre part. La situation est aggravée par l'absence de préparation de nombreuses entités à une crise cyber majeure : 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 des sauvegardes.

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).

Attaques indirectes (supply chain attack)

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 chaîne 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.

Vulnérabilités critiques

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 opérateurs d'importance vitale et des opérateurs de services essentiels ainsi que des 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.

IV. Adaptation de la posture Vigipirate « été - automne 2021 »

La posture Vigipirate « *été – automne 2021* »**, 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 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.

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 des commerces et activités 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.

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 sera accordé 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, 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, des aérogares ferroviaires ou routières, celle de l'aérogare de Metz-Nancy-Lorraine impose une vigilance attentive.

- *Spécificité du transport aérien*

Même si la pandémie affecte 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.

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 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 devra être 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 seront mises en place dans et aux abords des commissariats et des brigades de gendarmerie, notamment s'agissant des accueils.

Doivent être actualisés 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 les jours d'élections et 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 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. 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.

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),

- 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 services en charge de la gestion de crise en interministériel 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.

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.

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*

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 ;

- à la chaîne vaccinale contre la COVID-19.

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 présentée aux paragraphes supra (III) 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 31-09 - 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 effectuée.

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/.

V. 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 seront 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.

VI Sensibilisation des professionnels et du grand public

Malgré la crise sanitaire actuelle, 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, 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 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 :

Annexe 1 : Drones : Règles d'utilisation et mesures de prévention face à un usage malveillant

Annexe 2 : Fiche pratique prévention et signalement des cas de radicalisation djihadiste.

Le préfet,

Laurent Touvet