PRÉFET
DE LA MOSELLE
Liberté
Égalité
Fraternité

Cabinet
Direction des sécurités
Pôle sécurité intérieure

Metz, le 21 JUIN 2023

POSTURE VIGIPIRATE

La nouvelle posture Vigipirate « été - a*utomne 2023* » est active à compter du 21 juin 2023 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 en lien avec la coupe du monde de rugby ;
- la sécurité des lieux de rassemblement culturels et festifs ;
- la sécurité des transports et des bâtiments publics.

La coupe du monde de rugby se tiendra en France métropolitaine du 8 septembre au 28 octobre 2023 et constitue le principal enjeu sécuritaire de la période couverte par la présente posture.

Attentions particulières à la menace cyber dans le cadre de cette adaptation de la posture VIGIPIRATE « été - a*utomne 2023* » :

1 – l'invasion de l'Ukraine par la Russie, lancée le 24 février 2022, continue de représenter une menace pour les réseaux français. Depuis un an, l'Ukraine a subi de très nombreuses attaques informatiques visant à espionner et déstabiliser les systèmes d'information du pays. Ces attaques ont été majoritairement le fait d'acteurs liés aux services de renseignement russes, mais aussi de groupes hacktivistes pro-russes.

2 – les compétitions sportives internationales majeures font régulièrement l'objet d'attaques. Ces évènements constituent en effet une cible de choix pour des acteurs aux motivations diverses, qui peuvent chercher à conduire des actes malveillants pour des missions d'espionnage, dans un but lucratif, ou à des fins de déstabilisation.

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

- activation des mesures SAN 11-01 et SAN 21-01 (uniquement sur la période du 1er septembre au 1er novembre et dans les zones concernées par l'accueil de matchs de la CMR 23) :

SAN 11-01 : mise en alerte du dispositif de veille sanitaire et des capacités analytiques, notamment NRBC, pendant la coupe du monde de rugby ;

SAN 21-01 : mise en alerte des structures d'urgence des établissements de santé et de leurs structures de soins d'aval (plateau technique chirurgical, réanimation, etc).

- activation des mesures NUM 21-02 et NUM 31-06 (cf point 9 relatif à la sécurité du numérique) et extension des mesures RSB 12-01 et BAT 12-03 :

RSB 12-01 : renforcer la surveillance et le contrôle lors des rassemblements liés aux manifestations religieuses, politiques, sportives (coupe du monde de rugby) et culturelles (olympiades) et une vigilance accrue quant à la détention d'armes blanches, l'utilisation de voitures béliers contre les attroupements.

BAT 12-03 : durant la période de la coupe du monde de rugby, une attention particulière sera portée à la surveillance des lieux de rassemblements festifs, notamment les restaurants et débits de boissons ainsi qu'aux établissements de santé et aux évènements organisés dans le cadre des Olympiades culturelles.

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 2023*» est marquée par l'accueil de la coupe du monde de rugby et les flux importants de voyageurs dans les transports collectifs de personnes qui seront associés. En outre, plusieurs évènements sportifs servant de *test events* pour l'organisation des Jeux olympiques et paralympiques de Paris 2024 (JOP 24) seront organisés.

I. Adaptation de la posture Vigipirate « été - automne 2023 »

La posture Vigipirate « *été – automne 2023* », **maintient le territoire national au niveau « *sécurité renforcée - risque attentat* ».**

1 - Sécurité de la coupe du monde de rugby 2023

Bien qu'aucune menace majeure ciblant spécifiquement l'évènement n'ait été détectée à ce jour, la coupe du monde de rugby demeure une vitrine médiatique internationale et un vecteur de concentration de foules qui en font une cible privilégiée pour tous types d'individus ou groupes malveillants.

La Coupe du monde de rugby à XV (CMR 2023) se déroulera en France du vendredi 8 septembre au samedi 28 octobre 2023. La compétition réunira 20 équipes, représentant des nations issues de cinq continents, qui disputeront 48 matchs pendant cette période de 51 jours au total. L'affluence attendue pour ce *grand événement sportif international* (GESI) est estimée à 2,6 millions de spectateurs au total, dont 600 000 visiteurs étrangers présents sur le territoire national pour suivre la compétition. Par ailleurs, le nombre de téléspectateurs escomptés est évalué à 900 millions.

Les matchs seront organisés dans les villes-hôtes suivantes : Saint-Denis (93), Saint-Etienne (42), Bordeaux (33), Marseille (13), Toulouse (31), Lille (59), Nice (06), Nantes (44) et Lyon (69).

2 - 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.

3 - 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.

4 - 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

5 - 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.

6 - 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*

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

- l'organisation ministérielle et les liens entre services de l'Etat 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 avec les préfectures de départements, les collectivités territoriales et les opérateurs le cas échéant, 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* (PPMS, ou document assimilé) et des *plans de continuité d'activité* (PCA) à adapter en conséquence et la réalisation des exercices associés. En cas d'évènement perturbant le fonctionnement de l'établissement concerné (violences, intrusion, risque de débordement, etc.), 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 de personnels exerçant une mission de service public ou lors de diffusion d'informations relatives à sa vie privée, familiale ou professionnelle, conformément aux consignes adressées aux recteurs dans la circulaire du 9 novembre 2022 relative au plan pour la laïcité dans les écoles et établissements scolaires ;

- les séjours de cohésion dans le cadre du service national universel ;
- le maintien d'une haute vigilance à la sécurisation des systèmes d'information au regard de l'évaluation de l'ANSSI et des consignes relayées par le fonctionnaire de sécurité des systèmes d'information des *ministère de l'éducation nationale et de la jeunesse* MENJ/*ministère de l'enseignement supérieur et de la recherche* (MESR)/*ministère des sorts et de jeux olympiques et* paralympiques (MSJOP).

➢ *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 établissements du MSJOP mettront en œuvre les mesures des directives interministérielles.

Il importe également que des liens renforcés soient déployés entre les services de l'Etat 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 organismes des MENJ/MESR et du *ministère de l'agriculture et de la souveraineté alimentaire* (MASA) doivent maintenir leurs efforts habituels, et toujours indispensables, de sécurisation des personnes et des biens (personnels et usagers).

-Maintien d'une vigilance particulière des sites sensibles

Dans les établissements et les sites des opérateurs sous tutelle des MENJ/MESR et du MASA, une attention particulière sera portée à la protection et aux contrôles des laboratoires sensibles soumis à une réglementation spécifique, ainsi qu'aux lieux de stockage de matières dangereuses (sources radioactives, produits toxiques ou agents pathogènes, précurseurs d'explosifs, matières biologiques, etc.) et lieux abritant des animaleries.

Les zones considérées sensibles (zones à régime restrictif, zones sécurisées, zones d'accès restreint) doivent faire l'objet d'une vigilance maximale, de procédures de contrôle renforcées et de signalements systématiques.

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 *haut-fonctionnaire de défense et de sécurité* (HFDS) du périmètre ministériel dont relève son établissement.

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

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

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

Compte tenu de la situation internationale et de la persistance d'un niveau élevé de menace terroriste, les exploitants de sites touristiques sont invités à renforcer leurs mesures de vigilance et à prendre l'attache des forces de sécurité intérieure (police nationale et gendarmerie nationale). L'attention des propriétaires de monuments qui désirent participer aux 40èmes Journées européennes du patrimoine est tout particulièrement attirée sur les mesures de précaution élémentaires et la nécessité de se manifester auprès du commissariat de police ou de la brigade de gendarmerie locale. Concernant cet évènement particulier, les recommandations de vigilance accrue concernant les sites à forte valeur symbolique du point de vue historique régulièrement formulées dans le cadre de l'exploitation normale de ces monuments restent valables.

Pour ce qui concerne les événements se déroulant sur la voie publique, plus nombreux durant l'été, les organisateurs sont invités à se référer au guide des bonnes pratiques de sécurisation d'un événement de voie publique disponible sur le site Internet du ministère de l'Intérieur à l'adresse suivante :

https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenements-de-voie-publique

Ce document détaille les procédures de déclaration à respecter et donne des exemples illustrés de mesures de protection, contre les véhicules béliers notamment. Une série d'autres guides de recommandations est également disponible sur le site internet du SGDSN et listée dans la 6ème partie du présent document.

La période est également marquée par l'Olympiade culturelle dans le cadre de laquelle sont labélisés des évènements permettant de rappeler les liens qui existent entre le sport et la culture. Compte tenu de la couverture médiatique et de la puissance évocatrice des Jeux olympiques et paralympiques de Paris 2024, les organisateurs d'évènements labélisés sont invités à observer scrupuleusement les consignes formulées dans la présente note de posture.

Enfin, les sinistres récents au sein de bâtiments classés ou inscrits au titre des monuments historiques invitent les établissements culturels 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.

8 - 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 solidarités et de la santé d'autant plus à l'approche de la préparation des grands évènements sportifs internationaux se déroulant en France comme la Coupe du monde de rugby 2023, les jeux olympiques et paralympiques 2024 qui se dérouleront sur l'ensemble du territoire national d'ici à l'été 2024. Les établissements à proximité de sites sportifs où se dérouleront ces grands événements sportifs internationaux 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) ;
- les établissements de santé accueillant des mineurs dans le cadre du bilan somatique et médico-psychologique (conformément aux termes de l'instruction du 23 février 2018

relative à la prise en charge des mineurs de retour de zone d'opérations de groupements terroristes, notamment la zone irako-syrienne) ;

- les systèmes d'information qui sont des cibles régulières d'attaques du fait de leurs vulnérabilités. Le risque de cyberattaque est majoré par un état de la menace cyber préoccupant.

➢ *Secteur travail*

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

Ces agences et opérateurs veilleront à demeurer en contact avec les FSI locales dans un contexte où des individus pourraient profiter de la vitrine d'un grand événement sportif pour porter leurs revendications par des contestations éventuellement violentes.

9 - Sécurité du numérique

➢ *Contexte général*

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

➢ *Objectifs de sécurité recherchés sur la période*

L'évaluation de la menace pour la sécurité du numérique 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 21-02 (activée) : consulter régulièrement les sources d'information relatives aux vulnérabilités et attaques (site Internet du CERT-FR) :

Afin de se 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 SI.

Il est notamment possible de s'appuyer sur les bulletins du CERT-FR (https://www.cert.ssi.gouv.fr/avis/ et https://www.cert.ssi.gouv.fr/alerte/).

Cette veille sur les vulnérabilités doit être réalisée de manière quotidienne, idéalement via un processus automatisé à partir de sources complémentaires pour couvrir l'ensemble des briques du système d'information.

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 31.06 (activée) : sensibiliser les utilisateurs sur un risque de sécurité et un comportement à adopter :

Dans le contexte d'importance des menaces d'origine cyber, il convient de sensibiliser régulièrement les utilisateurs aux risques numériques et à l'application de la politique de sécurité des systèmes d'information, en particulier vis-à-vis de l'utilisation de support amovibles, de navigation Internet ou d'échanges de courriels.

L'attention à la sensibilité de l'information et à sa protection est également à intégrer au sein de cette sensibilisation. La non-séparation des usages et matériaux personnels et professionnels, échanges professionnels dans des lieux publics, présence de matériaux protégés ou classifiés sur des systèmes inadéquats sont à proscrire.

Dans le cadre de cette sensibilisation, il est possible de s'appuyer sur SecNumacadémie (https://secnumacademie.gouv.fr/), la formation en ligne de l'ANSSI, qui détaille les bonnes pratiques pour une utilisation sécurisée des outils numériques.

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 51-01 : vérifier les annuaires de crise et le fonctionnement des moyens de communication sécurisés :

Face aux menaces cyber, il est essentiel de vérifier que les annuaires de crise, contenant les contacts du personnel pertinent en cas de crise, en interne comme en externe, sont bien à jour et correctement diffusés à tous les acteurs. Par ailleurs, certaines menaces (notamment de type rançongiciel) peuvent aboutir à la perte des outils de communication usuels. Il est nécessaire de tester régulièrement les moyens de communication alternatifs et sécurisés, qui pourront être utilisés dans le cas d'une attaque impactant les outils de communication nominaux.

Des tests de vérification des communications peuvent être menés pour vérifier la bonne réception des alertes par les contacts d'urgence, ainsi que la capacité de chacun à utiliser les outils de connexion sécurisés.

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 - Signalement des cas suspects de radicalisation, des troubles comportementaux ou psychiatriques/psychologiques

La radicalisation se caractérise par un changement de comportement qui peut conduire certaines personnes à l'extrémisme ou au terrorisme. Des troubles psychologiques peuvent offrir un terreau favorable à la radicalisation. L'objectif du signalement au *centre national d'assistance et de prévention de la radicalisation* (CNAPR) est de protéger ces personnes contre elles-mêmes et la population contre de possibles comportements violents. Les combinaisons de comportements suivants doivent éveiller la vigilance 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 complotiste ou apocalyptique, tentative d'imposition agressive d'un ordre religieux.

Le signalement des cas suspects de radicalisation, quel que soit le type de radicalisation (religieuse, politique, etc.) se réalise de la manière suivante :

- Appel au numéro vert : 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.

Je rappelle l'existence d'un référent radicalisation/sécurité en préfecture qui a vocation à servir d'interlocuteur local pour cette problématique.

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. Les professionnels qui vendent ce type de produits ont l'obligation de signaler tout vol, disparition ou transaction suspecte au *plateau d'investigation explosif et armes à feu* (PIXAF) de la gendarmerie nationale, point de contact national.
/pixaf@gendarmerie.interieur.gouv.fr – 01 78 47 34 29 (24/7).

5 - 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 de sensibilisation sont accessibles en ligne depuis l'espace Vigipirate du site Internet du SGDSN (https://www.sgdsn.gouv.fr/vigipirate/les-affiches-de-sensibilisation). Elles 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. Aussi, ces affiches peuvent être téléchargées et imprimées sur un format adapté au lieu où elles sont placées afin de les rendre visibles 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 (https://www.sgdsn.gouv.fr/vigipirate/les-fiches-de-recommandation-et-de-bonnes-pratiques) :

- recommandations à l'attention des gestionnaires de parc et loueurs de véhicules (prévention des attaques au véhicule bélier) ;
- signalement des situations suspectes ;
- sécurisation de son établissement lors de journées portes-ouvertes ;
- organisation d'un confinement face à une menace terroriste ;
- signalement de tout vol ou utilisation suspecte de produits chimiques ;
- sécurité du numérique : l'hameçonnage (ou *phishing*) ;
- recommandations pour la sécurisation des lieux de rassemblement ouverts au public ;
- sécurité du numérique : sensibilisation des dirigeants ;
- se protéger contre les attaques au véhicule bélier ;
- préparer ses déplacements et voyages à l'étranger ;
- guide des bonnes pratiques pour la sûreté des espaces publics ;
- prévention et signalement des cas suspects de radicalisation ;
- règles d'utilisation des drones et mesures de prévention face à un usage malveillant ;
- chaîne d'alerte face à une menace.

En complément, plusieurs guides de bonnes pratiques, à destination des élus et des professionnels, sont également téléchargeables sur le site du SGDSN (https://www.sgdsn.gouv.fr/vigipirate/les-guides).

Le préfet,

Laurent Touvet