PRÉFET
DE LA MOSELLE
Liberté
Égalité
Fraternité

Metz, le 21 DEC. 2022

POSTURE VIGIPIRATE

VIGIPIRATE
SECURITE RENFORCEE
RISQUE ATTENTAT

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

La nouvelle posture Vigipirate « *hiver 2022 – printemps 2023* » est active et maintient l'ensemble du territoire national au niveau « sécurité renforcée - risque attentat ».

Cette posture Vigipirate adapte le dispositif en mettant 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).

En outre, la période considérée pourrait être potentiellement marquée par des délestages électriques, limités dans le temps et dans l'espace, susceptibles de faciliter les intrusions malveillantes dans les bâtiments et d'entraîner des difficultés provisoires pour contacter les numéros d'urgence à partir des lignes mobiles et/ou fixe.

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

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 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.

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.

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

II- Sécurité des grands espaces de commerce, de tourisme et de loisirs

Les lieux de commerce, les espaces de loisirs et les sites touristiques majeurs restent des cibles privilégiées. La sécurité doit être renforcée autour des grands espaces de rassemblements ayant pour objet des activités commerciales (centres commerciaux, salons d'expositions, foires, etc.). Les interconnexions de transports en milieu clos dotées de commerces (gares, etc.) demeurent également un point de vigilance.

Une vigilance accrue doit être observée 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 et d'hiver, marquées par une forte affluence, demeure un axe d'attention majeur.

De façon plus générale, si des éléments objectifs attestent d'une menace sur le plan local, ou qu'un événement révèle une vulnérabilité particulière, ils seront communiqués aux responsables de sûreté des établissements concernés afin de leur permettre d'adapter leur dispositif.

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

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

1- 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.

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

3- 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 et la préfecture de Moselle reste à votre disposition pour y travailler.

4- 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).
Par ailleurs, pour les espaces complexes le justifiant, le recours à la notion de « périmètre vidéoprotégé » peut-être utilement envisagé.

De même, à titre exceptionnel, la présence d'agents privés de sécurité, même itinérants, sur la voie publique, aux abords de leur site pourra être autorisée.

III- Sécurité des transports collectifs

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 et des réseaux de transport en commun doit être renforcé.
La menace visant les emprises des gares impose une vigilance quotidienne. Les couloirs de liaison intermodaux doivent faire l'objet d'une attention particulière.

Même si la pandémie impacte la fréquentation du transport aérien, la direction générale de l'aéroport de Metz-Nancy-Lorraine 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.

Les transports terrestres constituent toujours une cible d'intérêt, à la symbolique et l'impact forts, à l'instar de la récente attaque en Allemagne. En outre, la reprise progressive du trafic depuis plusieurs mois liée à la réduction des mesures sanitaires fait du secteur des transports une cible d'opportunité en raison notamment de la fragilité de cette reprise, des conséquences économiques et des impacts sur la population que pourraient avoir une attaque même de faible ampleur.

Toute information relative à une intrusion malveillante ou tentative de sabotage dans les infrastructures et les réseaux dédiés à la circulation des trains (voies ferrées classiques, lignes à grande vitesse, réseaux interurbains, etc.) doit faire l'objet d'une communication immédiate aux FSI locales. Chaque incident doit être considéré avec la plus grande attention et faire l'objet d'un compte-rendu vers le *centre ministériel de veille opérationnelle et d'alerte* (CMVOA) du ministère de la transition écologique : téléphone : 01 40 81 76 20 ; mèl : permanence.cmvoa@developpement-durable.gouv.fr

IV- Sécurité des bâtiments publics

Un effort particulier doit être porté à la protection des bâtiments publics. De même, des mesures renforcées de sécurité doivent être mises en place dans et aux abords des commissariats et des brigades de gendarmerie, notamment s'agissant des accueils.

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

Une vigilance particulière sera également portée aux bureaux de vote pendant la durée des élections mais aussi à la sécurité des palais de justice et des établissements pénitentiaires dans le contexte de procès dits « sensibles ». Elle sera renforcée lors des procès des personnes mises en cause pour faits de terrorisme.

Cette vigilance peut également concerner les structures de la protection judiciaire de la jeunesse (PJJ), qui prennent en charge des mineurs poursuivis pour association de malfaiteurs à but terroriste ; et les services pénitentiaires d'insertion et de probation (SPIP) 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.

V- 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

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

-les mesures de sécurisation nécessaires à prendre en 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, notamment en cas de délestages électriques ;

-la mise à jour des plans particuliers de mise en sûreté (ou document assimilé) et des plans de continuité d'activité à adapter en conséquences 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 ;

-le travail partenarial avec les acteurs concourant à la préparation des grands évènements sportifs internationaux se déroulant en France ;

-les séjours de cohésion dans le cadre du service national universel dont la prochaine édition débutera le 19 février 2023 ;

-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 MENJ/MESR/MSJOP.

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.

Par ailleurs, une vigilance devra être portée à la préparation des grands évènements sportifs.

Les mesures des directives ministérielles et interministérielles doivent être mises en œuvre au sein des établissements et organismes rattachés aux 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.

Les objectifs de sécurité recherchés durant la période

a - Sécurisation des personnes et des biens

- le renforcement des mesures de sécurisation en raison du contexte énergétique

Les coupures électriques qui pourraient éventuellement se produire cet hiver rendront les sites des MENJ/MESR/MSJOP vulnérables aux risques d'intrusion. Chaque responsable d'établissement ou organisateur d'activités relevant des ministères doit dès à présent étudier les contremesures contribuant au renforcement de la sécurisation des sites, avec une attention particulière sur les établissements disposant d'un internat et les sites sensibles. Ces mesures devront utilement être partagées avec les préfectures, les forces de sécurité intérieure, les services de secours ainsi que les collectivités territoriales.
Les mesures prévues en cas de coupure électrique doivent être inscrites dans le plan particulier de mise en sûreté (PPMS) ou dans le plan de continuité d'activité (PCA) de l'établissement. Les procédures doivent faire suite à une analyse des risques en fonction de l'ERP (classement, type, risques particuliers, environnement).
Maintien des consignes en vigueur
Les établissements et organismes des MENJ/MESR et du MASA doivent maintenir leurs efforts habituels, et toujours indispensables, de sécurisation des personnes et des biens (personnels et usagers).

Dans l'enseignement agricole, la vigilance des responsables d'établissements doit aussi porter sur les opérations de type « marchés de fin d'année de produits locaux » (dans les locaux de l'établissement ou en extérieur sur un marché de Noël) ainsi que sur tout déplacement d'apprenants (quelle que soit la destination).

-le 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. En situation de délestage électrique, il est indispensable d'organiser y compris hors jours et heures ouvrables la sécurité de ces sites les plus sensibles en tenant compte du fait que les portes de nombreux bâtiments vont s'ouvrir (au-delà de la durée assurée par les dispositifs de secours). Il importe par ailleurs d'organiser le dispositif de mise en sécurité d'équipements et dispositifs expérimentaux les plus sensibles aux coupures d'énergie non programmées.
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.

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

Les services et établissements des MENJ/MESR/MSJOP doivent veiller à :

-réduire et mieux maitriser l'exposition sur Internet de services de connexions à distance à usage d'administration, pédagogique ou de recherche. En particulier, les services d'accès distants largement déployés pendant les confinements liés à la crise sanitaire doivent faire l'objet d'une réévaluation ;
-mener des actions de renforcement de la sécurité des annuaires électroniques afin de réduire les risques de diffusion de rançongiciels ;
-s'assurer de la complétude des politiques de sauvegardes informatiques et des capacités à disposer de sauvegardes déconnectées résistantes aux rançongiciels ;

-élaborer des plans d'arrêt maitrisés et de redémarrage des centres d'hébergements de serveurs, afin de limiter les risques de pertes de données en lien avec les possibles délestages électriques territoriaux ;
-protéger au niveau adéquat les locaux dédiés à l'hébergement des systèmes d'information, des stockages de données et des systèmes de restauration ;
-poursuivre la sensibilisation régulière des apprenants et des personnels aux menaces cyber et aux bonnes pratiques à adopter au quotidien, en particulier sur les menaces relatives au hameçonnage (*phishing*) ;
-poursuivre les campagnes récurrentes de renouvellement des mots de passe de tous les usagers en prenant en compte les nouveaux standards édictés par l'ANSSI et la CNIL ;
-maintenir une politique active des mises à jour de sécurité des applications et infrastructures numériques ;
-remonter systématiquement les incidents significatifs de sécurité numérique auprès du responsable de la sécurité des systèmes d'information du périmètre concerné, qui est en lien avec les acteurs de réponse et d'appui aux incidents.

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

Le contexte international et les tensions s'exprimant sur le territoire national invitent à maintenir un haut niveau de vigilance notamment pour les établissements recevant du public et les écoles et conservatoires relevant du ministère de la Culture.
A l'approche des jeux olympiques et paralympiques de Paris se déroulent sur l'ensemble du territoire national et d'ici à l'été 2024 une série d'événements culturels labellisés Olympiades culturelles. Ces événements en plus de la valeur symbolique inhérente aux sites retenus et aux actions de démocratisation culturelle, peuvent s'avérer particulièrement exposés à la menace terroriste du fait de leur association au mouvement olympique.
Les acteurs culturels sont d'une manière générale invités à appliquer les mesures de prévention répertoriées dans les guides pratiques disponibles en ligne (http://www.culture.gouv.fr/Actions-de-renforcement-et-de-surveillance-des-lieux-culturels). Ils sont ainsi invités à renforcer leurs mesures de vigilance et à prendre l'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.
Enfin, les gestionnaires sont invités à prendre en compte les conséquences potentielles d'une interruption de la fourniture de l'électricité sur leurs systèmes de sécurité et les ajustements nécessaires en matière de mesures et de procédures de sécurité. La mise à jour des plans de continuité est vivement conseillée.
En matière de cyber sécurité, les tensions internationales actuelles accroissent le niveau de menace déjà élevé en lien avec les attaques de type criminel (rançongiciels par exemple) exploitant notamment des vulnérabilités critiques. Les acteurs culturels sont invités à la plus grande prudence et à appliquer les préconisations de l'agence nationale de sécurité des systèmes d'information (ANSSI).

VII - Sécurité des établissements de santé, sociaux et médico-sociaux

Les opérateurs des ministères sociaux, qu'il s'agisse des champs santé, solidarités ou travail, demeurent des cibles vulnérables. En effet, plusieurs thématiques et projets de réforme sensibles pourraient amener des individus malintentionnés à commettre des actes de nature terroriste. La vigilance doit en conséquence demeurer élevée pour les opérateurs des champs précités.

La probabilité d'un délestage électrique sur la période hiver-printemps 2023 nécessite également aux opérateurs des ministères sociaux une attention toute particulière. Leur vulnérabilité pourrait être accrue en cas de défaut d'alimentation électrique de leurs équipements et dispositifs de sécurité.

1 - Objectifs de sécurité recherchés sur la période

Poursuite des actions mises en œuvre par les forces de sécurité intérieure :

-la sécurisation des abords des établissements de santé ;
-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 la santé et de la prévention. Les directeurs d'établissement de santé s'assurent également de l'effectivité de la mise en œuvre des mesures de sûreté de leur plan de sécurisation d'établissement (PSE).

2 – Points 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.

3 - Point de vigilance

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, dans le contexte des réformes gouvernementales à venir au printemps 2023.
Ces agences et opérateurs veilleront, dans un probable contexte de contestations violentes, à demeurer en contact avec les FSI locales en cas de tensions et de contestations violentes.

VIII – Mesures de sécurité du numérique (ANSSI) à appliquer par les responsables de la sécurité des services informatiques des administrations et des entreprises privées.

L'invasion de l'Ukraine par la Russie, lancée le 24 février 2022, continue de représenter une menace pour les réseaux français. Les menaces visant les administrations et les entreprises privées restent élevées et variées (attaques par rançongiciels, attaques indirectes et vulnérabilités critiques).

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

-Mesure NUM 11-02 - Rechercher sur le SI des marqueurs particuliers correspondant à une attaque

Compte tenu des campagnes d'exploitation des vulnérabilités sur les services Microsoft, il est recommandé de prendre connaissance des marqueurs de compromissions publiés ou transmis par l'ANSSI et indiquer à l'ANSSI le résultat de la recherche et ses modalités.

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

Compte tenu des attaques menées par déni de service (DDOS), il est important de s'assurer que les opérateurs de services numériques 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.

-Mesure NUM 41.01 - Valider et appliquer un correctif de sécurité

Face aux vulnérabilités critiques, il est important d'appliquer au plus tôt 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. A noter que l'exploitation de certaines de ces vulnérabilités permet l'accès à des comptes privilégiés pour l'attaquant et étend ses capacités de latéralisation sur les systèmes. La période de fin d'années peut également donner lieu chez les opérateurs privés à une stabilisation et une limitation des mises à jour des infrastructures, pouvant exposer certains systèmes d'information à des failles sur la période.

-Mesure NUM 51-02/52-02 - Adapter les dispositifs de réponse à incidents aux caractéristiques de la menace

Compte tenu des menaces cyber persistantes, 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, 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 réussit :

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

-Mesure NUM 51-01 - Vérifier les annuaires de crise et le fonctionnement des moyens de communication sécurisés (nouvelle mesure activée)

Face aux menaces cyber, il convient de s'assurer que la capacité de communication entre le personnel en charge de répondre à la crise sera maintenue. Il est donc 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 51-05 – Réaliser des tests de restauration des sauvegardes (nouvelle mesure activée)

Afin de s'assurer de la capacité d'une reprise rapide de l'activité en cas d'attaque destructive et d'entraîner les équipes en charge de ces opérations, il convient d'organiser régulièrement des tests de restauration des sauvegardes réalisées sur les systèmes d'information. Ces tests, qui doivent être effectués sur les sauvegardes en ligne et hors-ligne, sont une opportunité de vérifier la présence des sauvegardes, leur qualité et l'aptitude à restaurer un système d'information à partir de ces dernières.

Le guide « d'hygiène numérique » de l'ANSSI apporte des précisions vis-à-vis de la mise en place de politiques de sauvegarde et de réalisation des tests :

https://www.ssi.gouv.fr/uploads/2017/01/guide _hygiene_informatique_anssi.pdf

IX - Consignes particulières de vigilance, prévention et protection

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. Leurs hiérarchies respectives doivent s'assurer que les mesures de sécurité sont appliquées.

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 ;

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).

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 mon autorité, 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, assurer le conseil auprès des autorités requérantes et d'informer les hautes autorités en charge de la préparation et de la réponse de l'Etat face à un événement terroriste NRBC.

Rappels des consignes NRBC aux services intervenants

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

Pour cela, il se révèle indispensable de :

-contrôler la diffusion et la connaissance des consignes NRBC auprès des agents qui auraient à les mettre en œuvre (fiches réflexes, instructions et circulaires, participation aux formations et entraînements interministériels) ;

-rappeler les consignes de protection et les conduites à tenir individuelles et collectives ;

-déplacer, si nécessaire, certains moyens NRBC vers les sites de grands rassemblements du public : lots PRV NRBC, unités mobiles de décontamination. En cas de déplacement de ces moyens NRBC, il est nécessaire, dans cette zone, d'activer la fiche ALR 22.05 (assurer la disponibilité des tenues de protection et moyens NRBC dans les véhicules des services de secours et d'aide médicale d'urgence, ainsi qu'auprès des personnels de la police, de la gendarmerie ou des unités militaires amenées à intervenir).

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.

X - Sensibilisation du grand public

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

1 - Efforts de communication

Les services de l'Etat et collectivités veilleront à ce que les opérateurs publics et privés situés dans leur champ de compétence mettent en place les logogrammes : **« *Sécurité renforcée – risque attentat* ».**

Ces logogrammes peuvent être téléchargés sur le site :
-du gouvernement http://www.gouvernement.fr/vigipirate ;
-du SGDSN http://www.sgdsn.gouv.fr/vigipirate .

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, les fiches renouvelées de sensibilisation à destination, tant du grand public que des professionnels, sont accessibles en ligne depuis l'espace Vigipirate du site internet du SGDSN.

Elles sont également sur l'espace dédié du site du gouvernement :

http://www.gouvernement.fr/risques/le-citoyen-au-coeur-du-nouveau-dispositif-vigipirate.

Par ailleurs, un ensemble de guides et bonnes pratiques, à destination des professionnels et des particuliers, est mis à disposition sur le site précité, ainsi que sur :

http://www.gouvernement.fr/reagir-attaque-terroriste

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

Enfin, le SGDSN a développé, en liaison avec de nombreux partenaires, une plateforme de sensibilisation Vigipirate qui se veut un outil pédagogique accessible au plus grand nombre. Cette plateforme s'appuie en particulier sur le document « *Faire Face Ensemble* » de 2016 mais aussi sur les guides de bonnes pratiques destinés aux professionnels. Elle intègre des témoignages vidéo, de citoyens ou de professionnels, ayant été confrontés à des attaques ou à des prises d'otages, ou dont les services contribuent au quotidien à lutter contre le terrorisme. Elle permet, en quelques heures, d'être sensibilisé à la menace terroriste et d'avoir une meilleure connaissance des gestes et réflexes à adopter afin de prévenir un acte terroriste ou de réagir en cas d'attaque.

3 Les comportements et gestes d'urgence

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 le site précité.

Le préfet,
Pour le préfet et par délégation,
Le sous-préfet de Forbach-Boulay,

Bruno Charlot