PRÉFET
DE LA MOSELLE
Liberté
Égalité
Fraternité

Metz, le 14 JAN. 2024

POSTURE VIGIPIRATE

VIGIPIRATE
SECURITE RENFORCEE
RISQUE ATTENTAT

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

La nouvelle posture Vigipirate « *hiver – printemps 2024* » est active et ramène 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 bâtiments à usage d'enseignement et des lieux de culte ;
- la sécurité des rassemblements festifs, culturels et religieux ;
- la sécurité des transports et des bâtiments publics et institutionnels.

La présente posture prévoit :

- l'**activation** des mesures **NUM 11-01**, **NUM 51-02/52-02** et **NUM 51-05 (pages 7 à 9)**;
- le **maintien** de la mesure **FRT 21-01** (activée le 13 octobre 2023) ;
- la **désactivation** des mesures **SAN 11-01**, **SAN 21-01**, **NUM 51-01** et **NUM 51-06** ;
- la **prolongation de l'extension** des mesures **BAT 12-01** et **BAT 12-03** aux établissements scolaires, d'enseignement supérieur et de recherche et aux lieux de culte (extension décidée le 13 octobre 2023) ;

La période des JOP, précédée de l'arrivée sur le territoire national de la flamme olympique fera l'objet d'une posture Vigipirate particulière, qui devrait être activée à compter du 1er mai 2024.

Toutefois, plusieurs *test events* et évènements promotionnels préalables aux JOP 2024 seront organisés dans la période couverte par la présente posture. Ils devront faire l'objet d'un effort particulier de sécurisation.

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.

Conformément à l'intitulé des mesures BAT 12-01, BAT 12-03 et RSB 12-01, la sécurité sera renforcée autour des lieux de culte avec un effort sur la présence visible des forces de l'ordre selon un mode de sécurisation dynamique, assorti de prises de contact avec les responsables de lieux de culte, voire statique (avant et pendant les offices et jusqu'à dispersion des fidèles) s'agissant des sites signalés comme sensibles voire très sensibles par les autorités religieuses. En liaison avec les autorités religieuses locales, la mise en œuvre de mesures de contrôle des accès (limitation du nombre d'accès, contrôles visuels des flux entrants à la diligence des équipes communautaires ou paroissiales) est recommandée. De la même façon, une attention particulière devra être portée aux véhicules en stationnement à proximité des lieux de rassemblement ou de culte. A cet égard, les maires seront sensibilisés à la nécessité de prendre des mesures temporaires d'interdiction de circuler et de stationner. Les militaires de l'opération Sentinelle pourront appuyer le dispositif de forces de l'ordre dans le cadre de la mesure BAT 13-04.

Les lieux sujets à de fortes affluences saisonnières durant les vacances scolaires (stations de sports d'hiver, salles de spectacles, etc.) bénéficieront de moyens adaptés. Les forces de sécurité intérieure et 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 nationales.

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.

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. 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 :

- l'évaluation des mesures de sécurisation renforcée des établissements et activités relevant des MENJ/MESR/MSJOP, avec le concours des forces de sécurité intérieure ;
- le maintien du niveau de vigilance face aux messages d'alerte à la bombe avec levée de doute systématique en lien avec les forces de sécurité intérieure ;
- l'organisation ministérielle et les liens entre services de l'Etat et opérateurs dans le cadre des JOP 24 ;

- le maintien d'une haute vigilance quant 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 ministères de l'éducation nationale et de la jeunesse MENJ/ministère de l'enseignement supérieur et de la recherche (MESR)/ministère des sports et des jeux olympiques et paralympiques (MSJOP).

Les objectifs de sécurité recherchés durant la période

a - Sécurisation des personnes et des biens

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. L'attentat du 13 octobre 2023 à Arras confirme la sensibilité forte de ces établissements.

Pour chacun de ces établissements, les mesures de sécurisation relevant des directives ministérielles et interministérielles, déjà déployées, doivent être maintenues au niveau Vigipirate « urgence attentat », en lien avec les forces de sécurité intérieure ainsi que les collectivités territoriales si nécessaire.

Une attention particulière est également portée aux établissements accueillant ces mêmes publics (centres régionaux des œuvres universitaires et scolaires, structures d'accueil collectif de mineurs, séjours de cohésion dans le cadre du service national universel) qui mettent également en œuvre les mesures de sécurisation adaptées à leur fonctionnement.

Toute mesure jugée utile doit être mise en œuvre. Le partage d'information et les procédures d'alerte sont à actualiser et à renforcer entre les relais des MENJ/MESR/MSJOP (cabinets de recteurs, fonctionnaires sécurité défense, responsables sécurité-sûreté, etc.), et les forces de sécurité intérieure.

L'enjeu sécuritaire et médiatique des JOP 24 appelle une organisation adaptée du MSJOP. Une haute vigilance des impacts des grands évènements sportifs sur le périmètre MSJOP devra être assurée, en lien notamment avec l'organisation interministérielle de suivi des JOP (CNCS, CIC notamment) et l'opérateur Paris 2024.

Les régions académiques et établissements du MSJOP mettront en œuvre les mesures des directives interministérielles et ministérielles. Il importe également que des liens renforcés soient déployés entre ces structures, les préfectures et les collectivités territoriales hôtes afin d'organiser le partage d'informations et de gestion d'incidents ou d'évènements graves.

Les établissements relevant du MSJOP identifiés comme sensibles dans le cadre des JOP 24 prendront l'attache des préfectures afin qu'une évaluation de la mise en sûreté soit assurée et les processus d'échanges d'informations en cas d'évènements graves consolidés.

b - 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.

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.

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

La persistance de la situation conflictuelle au Proche-Orient et les tensions s'exprimant sur le territoire national invitent à maintenir un haut niveau de vigilance pour les établissements recevant du public ainsi que les écoles et conservatoires relevant du ministère de la Culture. Ceux-ci sont parfois directement affectés par la recrudescence d'actes présumés antisémites et des actions malveillantes comme de fausses alertes à la bombe.

Par ailleurs, à l'approche des jeux olympiques et paralympiques de Paris, se déroule – sur l'ensemble du territoire national et d'ici à l'été 2024 – une série d'événements culturels labellisés « Olympiade culturelle » (parcours de la flamme en Moselle au mois de juin 2024). Or, ces derniers, en plus de la valeur symbolique inhérente aux sites retenus et aux actions de démocratisation culturelle, sont particulièrement exposés à la menace terroriste du fait de leur association au mouvement olympique.

Enfin, en matière de cyber sécurité, la vigilance doit être maintenue compte tenu du risque croissant d'attaques de nature criminelle susceptibles de porter atteinte au bon fonctionnement et à l'image des directions, services et établissements du ministère de la Culture.

Pour ce qui concerne les événements se déroulant sur la voie publique, 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.

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.

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) d'autant plus à l'approche des jeux olympiques et paralympiques 2024.

2 – Points d'attention

-les opérateurs d'importance vitale (vigilance sur la mise à jour des documents de planification dans la perspective des JOP24) ;
-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.

En conséquence, ces agences et opérateurs veilleront à mettre à jour la documentation relative à leur sécurisation dans la perspective des JOP24. En effet, des individus pourraient profiter de la vitrine de cet événement sportif international pour porter leurs revendications par des contestations éventuellement violentes.
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.

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

- https://www.cyber.gouv.fr (site de l'Agence nationale de la sécurité des systèmes d'information) ;
- https://www.cert.ssi.gouv.fr (site du centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques).

Au regard de l'évaluation de la menace pour la sécurité du numérique il est nécessaire d'appliquer les objectifs et mesures de sécurité suivants :

- **Mesure NUM 11-01 (activée) : déterminer l'ensemble des composants du SI contenant un logiciel/matériel particulier**

Le cycle de vie des équipements et applicatifs informatiques conduit à l'émergence de vulnérabilités susceptibles de conduire à la compromission des systèmes d'informations. Par ailleurs, certains éditeurs de solutions informatiques arrêtent la maintenance de technologies moins récentes, laissant ces technologies sans mise à jour disponible pour corriger d'éventuelles vulnérabilités.

Il est donc nécessaire de cartographier régulièrement son SI et les technologies le composant afin de pouvoir agir en cas de vulnérabilité et de fin de support d'une solution informatique. Cette cartographie doit permettre, à terme, d'identifier les composants du SI directement sous contrôle et ceux sous-traités. Ces travaux permettent de traiter plus efficacement les incidents de sécurité.

L'ANSSI propose un guide permettant de mettre en place un processus de cartographie des SI (https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation). Un exemple récent de ce phénomène est la fin du support de WINDOWS SERVER 2012 et 2012 R2. Ce système d'exploitation pour serveur répandu n'est plus supporté par l'éditeur Microsoft depuis le 10 octobre 2023. Il est donc nécessaire d'identifier la présence de ce système d'exploitation sur son système d'information et de lancer un projet de migration vers une version supportée, et d'isoler à minima les serveurs impossibles à migrer à date.

- **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 numériques, il est recommandé de prendre connaissance des marqueurs de compromissions publiés par l'ANSSI via les rapports de la menace (https://www.cert.ssi.gouv.fr/cti/) ou au travers du *feed* MISP public mis à disposition par l'ANSSI (https://misp.cert.ssi.gouv.fr/feed-misp). Ces marqueurs peuvent être complétés par d'autres sources de marqueurs provenant de partenaires de confiance.

Dans la mesure du possible, il convient d'ajouter ces marqueurs aux systèmes de détection disponibles (antivirus, EDR, NIDS, HIDS, etc.). Par ailleurs, il est recommandé de chercher la présence de ces marqueurs sur l'historique des journaux disponibles afin d'identifier d'éventuelles tentatives de compromission.

- **Mesure NUM 21-02 : 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 (déni de service distribué), il est important de s'assurer que les opérateurs de services numériques, d'une part, disposent d'infrastructures et composants de sécurité permettant d'absorber le trafic et qu'ils puissent transmettre à leurs clients une liste d'adresses IP illégitimes à bloquer et d'autre part, qu'ils assurent le renforcement de leurs systèmes d'information et des sites web hébergés. L'ANSSI a récemment publié une fiche pratique sur la mise en place d'un service de protection anti-DDoS, disponible sur son site web (https://cyber.gouv.fr/publications/les-denis-de-service-distribues-ddos).

Sur la base des informations transmises par l'ANSSI, il est nécessaire d'identifier les moyens de filtrage les plus efficaces (par exemple avec un équipement en entrée de réseau ou avec l'appui d'un opérateur de communication électronique ou un fournisseur de solution spécialisé). Il est recommandé de prendre en compte les différentes typologies d'attaques par déni de service (au niveau applicatif, spécifique à protocole ou basé sur la volumétrie) et la couverture offerte par les moyens de filtrage. Il vous revient ensuite de mettre en place ces mécanismes de protection anti-déni de service sur les infrastructures qu'ils hébergent ou demander la mise en place auprès des prestataires d'hébergement ou de communication le cas échéant.

- **Mesure NUM 31.06 : sensibiliser les utilisateurs sur un risque de sécurité et un comportement à adopter**

Dans le contexte d'importance des menaces d'origine cyber, il est nécessaire 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 supports 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.

En complément, les utilisateurs privilégiés doivent être particulièrement sensibilisés aux bonnes pratiques afin de réduire les risques cyber. Les différents guides de l'ANSSI émettent de nombreuses recommandations en ce sens, qu'elles portentsur l'administration sécurisée des systèmes d'information :

(https://cyber.gouv.fr/publications/recommandations-relatives-ladministration-securisee-des-systemes-dinformation), de systèmes reposant sur l'Active Directory

(https://cyber.gouv.fr/publications/recommandations-pour-ladministration-securisee-des-si-reposant-sur-ad)

ou lors la mise en place de politique de mots de passe :

(https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe).

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 et à l'état de la menace, il est impératif d'appliquer, dans les plus brefs délais, les correctifs de sécurité mentionnés dans les bulletins d'alerte de sécurité du CERT-FR. Les correctifs référencés dans les alertes doivent, si cela est nécessaire et pour des raisons d'urgence et de criticité, être appliqués en dehors des processus de maintien en condition de sécurité des systèmes d'information. De même, les correctifs mentionnés dans les avis de sécurité et qui correspondent à la veille sur plus d'une centaine de produits, doivent également être appliqués dans le cycle habituel de maintien en condition de sécurité des systèmes d'information. L'exploitation de certaines des vulnérabilités référencées permet l'accès à des comptes privilégiés pour l'attaquant et étend ses capacités de latéralisation sur les systèmes. La bonne application des correctifs de sécurité référencés doit être régulièrement contrôlée et validée. Les bulletins d'alerte de sécurité et les avis de sécurité sont disponibles sur le site https://ww.cert.ssi.gouv.fr.

Les correctifs de sécurité et alertes du CERT-FR mentionnés ci-dessous doivent impérativement être appliqués pour corriger des vulnérabilités récentes particulièrement critiques :

- Vulnérabilités sur les équipements de sécurité en bordure des réseaux (alertes CERTFR-2023-ALE-008, CERTFR-2023-ALE-004 et CERTFR-2022-ALE-013 du CERT-FR)

De nombreux équipements comme les pares-feux et les passerelles VPN sont régulièrement la cible des attaquants qui continuent de trouver des vulnérabilités leur permettant de les compromettre en prendre pied dans le SI ou d'obtenir des secrets d'authentification pour usurper l'identité des utilisateurs. Pour certains produits, les vulnérabilités remontent à 2018 et continuent d'être exploitées. Les utilisateurs doivent impérativement mettre à jour ou faire mettre à jour ces équipements et procéder au renouvellement régulier des secrets d'identification (procédure extrêmement lourde) ou basculer sur des solutions d'authentification à multiples facteurs :

- Vulnérabilités sur les systèmes industriels (CVE-2023-39979 (MOXA), CVE-2023-29130 (Siemens), CVE-2023-29411 et CVE-2023-29411 (CVE-2023-29412)

Certains équipements, comme des automates programmables, sont exposés sur Internet sans aucune mesure de sécurité. Ces équipements particulièrement vulnérables peuvent être manipulés à distance par des attaquants afin de compromettre les réseaux industriels. En tant qu'utilisateurs de ces systèmes vous devez vérifier la nécessité de maintenir une accessibilité de ces équipements à distance et, si cela s'avère le cas, mettre en place les mesures permettant de limiter l'accès à ces équipements par les seuls acteurs ayant besoin de s'y connecter (équipements de filtrage, réseau privé virtuel, lien réseau dédié).

- **Mesure NUM 51-02/52-02 (activée) : adapter les dispositifs de réponse à incidents aux caractéristiques de la menace**

Afin de garantir la plus grande réactivité et efficacité à un incident de sécurité informatique, il est nécessaire de construire un dispositif de réponse adéquat. En particulier, l'identification des ressources humaines en mesure d'armer les centres opérationnels de réponse est nécessaire, en passant si besoin par la contractualisation de *prestataires de réponse aux incidents de sécurité* (PRIS) pour renforcer l'action des équipes internes.

En complément, la définition d'une procédure-cadre de gestion des incidents ainsi que de fiches-réflexes pour les scénarios d'attaques les plus pertinents pour l'organisation (chiffrement d'un poste, DDoS, exfiltration de données, etc.) permettent de mettre en œuvre rapidement la réponse à incident, et donc d'en réduire la portée de manière significative.

Enfin, vous devez également vérifier qu'un plan de continuité d'activité (PCA), détaillant les besoins de continuité de votre centre opérationnel, existe et puisse être mobilisé pour assurer la continuité de la réponse en cas d'incident, même de nature non-cyber (disfonctionnement électrique, télécoms, indisponibilité bâtimentaire, etc.). Les moyens de continuité identifiés via le PCA doivent être vérifiés par vos soins via des tests et des exercices afin de vous assurer de leur parfaite disponibilité et efficacité en cas d'incident les mobilisant.

- **Mesure NUM 51-05 (activée) : réaliser des tests de restauration des sauvegardes**

Afin de garantir une reprise rapide de l'activité en cas d'attaque destructive et d'entraîner les équipes en charge de ces opérations, vous devez 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://cyber.gouv.fr/publications/guide-dhygiene-informatique.

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 ;

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.

Des actions de sensibilisation sont conduites au sein de la fonction publique (cf. guide de la prévention de la radicalisation de la fonction publique-DGAFP 2019/ lois et principes de la République). Je vous rappelle l'existence d'un référent radicalisation en préfecture (cabinet) qui a vocation à servir d'interlocuteur local pour cette problématique.

Le récent attentat à Paris le 2 décembre (pont de Bir Hakeim) a mis en exergue le profil d'un individu déjà condamné pour terrorisme, sorti en 2020 de détention, et sujet parallèlement à des troubles du comportement. Les troubles du comportement font l'objet d'une attention toute particulière et de dispositifs d'évaluation et de prise en charge *ad hoc* portés, notamment, par les circulaires Intérieur - Santé du 26 avril 2021 et 28 octobre 2022, avec des rappels réguliers.

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

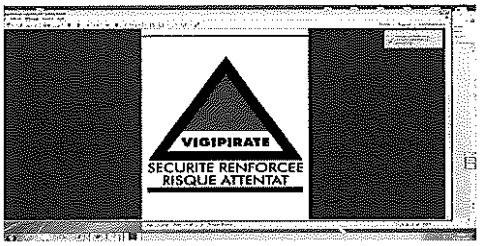
L'utilisation des drones est un mode d'action régulièrement mis en œuvre pour capter des images ou diffuser des messages mais qui peut évoluer vers des actes de malveillance ou terroristes. A l'occasion de grands rassemblements, les organisateurs doivent prendre en compte cette menace en sollicitant l'avis des référents sûreté locaux de la police ou de la gendarmerie nationales.

X - Sensibilisation du grand public

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

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, 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 doivent 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 et salles d'attente).

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

3 Les modules de formation en ligne

Deux modules de formation en ligne, développés en liaison avec de nombreux partenaires, sont accessibles (https://vigipirate.gouv.fr) :

- un module long, dédié essentiellement aux professionnels de la sécurité ;
- un module court, prochainement disponible en plusieurs langues, dédié au grand public.

Ces modules intègrent notamment 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. Ils permettent, 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.

Le préfet,

Laurent Touvet