Trois annexes non protégées :
extraits de l'adaptation de la posture interministérielle Vigipirate « Eté - automne 2023 »
en vigueur à compter du 21 juin 2023

Annexe 1 : extraits de l'évolution du contexte juridique concernant les ministères (MENJ, MESR et MSJOP)

– **Loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur (LOPMI)**

Le texte confie notamment la gestion des crises graves aux préfets qui dirigeront désormais l'action des établissements et services déconcentrés qui ne relèvent pas de leur autorité en temps normal.

Il institue chaque année une journée nationale obligatoire dédiée aux risques majeurs et aux gestes qui sauvent.

Enfin, en vue de la Coupe du monde de rugby en 2023 et des Jeux Olympiques de 2024, 11 nouvelles unités de forces mobiles (UFM) spécialisées vont être constituées.

– **Décret n° 2022-1397 du 2 novembre 2022 portant application de l'article L. 6224-1 du code des transports, relatif au régime encadrant la captation et le traitement des données recueillies depuis un aéronef dans certaines zones**

Le décret, entré en vigueur le 1er janvier 2023, détermine les autorités administratives délivrant les autorisations permettant la captation, l'enregistrement, la transmission, la conservation, l'utilisation ou la diffusion de données recueillies, depuis un aéronef, par un appareil photographique ou cinématographique ou par tout autre capteur de télédétection des zones interdites de captation aérienne de données. Il modifie et abroge les dispositions réglementaires en vigueur.

– **Décret n° 2023-204 du 27 mars 2023 relatif au brouillage des aéronefs circulant sans personne à bord**

Ce décret détaille certaines modalités d'application du brouillage des drones présentant une menace. En dehors des besoins de la défense nationale, c'est généralement le préfet qui autorise le recours au brouillage. La protection d'un site ou d'une manifestation particulièrement sensible nécessitera de faire appel aux forces de sécurité intérieure, ou à l'armée de l'air et de l'espace lors des événements justifiant le déploiement d'un dispositif particulier de sûreté aérienne.

– **Décret n°2023-255 du 6 avril 2023 autorisant la création d'un traitement automatisé de données à caractère personnel relatif à la prise en charge des mineurs de retour de zones d'opérations de groupements terroristes (MRZGOT)**

Annexe 2 : nouvelles mesures de la posture Vigipirate « Eté – automne 2023 »

1. Sécurisation des établissements d'enseignement et de recherche, des structures d'accueil collectif de mineurs (ACM), des séjours de cohésion du SNU et des établissements publics et activités relevant du ministère des sports et des jeux olympiques et paralympiques (MENJ/MESR/MSJOP)

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 pour 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 à prendre avec les préfectures de départements, les collectivités territoriales et les opérateurs, face aux risques d'intrusion ou de toute atteinte à la sûreté d'un établissement ;
- La mise à jour des *plans particuliers de mise en sûreté* (PPMS, ou document assimilé) et des *plans de continuité d'activité* (PCA) et la réalisation des exercices associés[1] ;
- Le signalement aux forces de sécurité intérieure de toute menace proférée à l'encontre de personnels exerçant une mission de service public ou de diffusion d'informations relatives à leur vie privée, familiale ou professionnelle[2] ;
- Les séjours de cohésion dans le cadre du service national universel ;
- La vigilance sur la sécurisation des systèmes d'information.

Contexte général

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

Objectifs de sécurité recherchés durant la période

- **Coupe du monde de rugby 2023**

L'enjeu sécuritaire et médiatique de la coupe du monde de rugby appelle une organisation adaptée du MSJOP et une vigilance soutenue et des liens renforcés entre services de l'Etat et collectivités territoriales.

- **Sécurisation des personnes et des biens**

- Maintien des consignes en vigueur

Les établissements et organismes des MENJ/MESR/MSJOP et du MASA doivent maintenir leurs efforts de sécurisation des personnes et des biens (personnels et usagers)[3].

---

[1] Pour rappel, tous les écoles et établissements scolaires doivent avoir réalisé leur exercice « attentat-intrusion » avant la fin d'année scolaire 2022-2023.

[2] https://www.education.gouv.fr/bo/22/Hebdo42/MENG2232014C.htm

[3] - l'élaboration et/ou la mise à jour des diagnostics de sûreté et des plans particuliers de mise en sûreté (PPMS) ou documents similaires et la réalisation des exercices associés à ces PPMS ;

- Maintien d'une vigilance particulière des sites sensibles

Une attention 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 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.

Le fonctionnaire de sécurité de défense/ officier de sécurité (OS) de l'établissement doit être informé de toute risque et incident et en faire part au HFDS ministériel.

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

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

2. Sécurité de la coupe du monde de rugby 2023 (MIOM)

La coupe du monde de rugby (CMR 2023) demeure une vitrine médiatique internationale et un vecteur de concentration de foules.

Elle se déroulera en France du vendredi 8 septembre au samedi 28 octobre 2023. Elle réunira 20 équipes, qui disputeront 48 matchs pendant 51 jours au total. L'affluence attendue est estimée à 2,6 millions de spectateurs, dont 600 000 visiteurs étrangers. Le nombre de téléspectateurs escomptés est évalué à 900 millions. Les matchs seront organisés à : Saint-Denis (93), Saint-Etienne (42), Bordeaux (33), Marseille (13), Toulouse (31), Lille (59), Nice (06), Nantes (44) et Lyon (69).

En novembre 2022, des directives ont été transmises aux préfets pour organiser la protection de la CMR (sites, "villages rugby" et autres manifestations publique) :

- L'instruction (NOR : IOMA2223363J) du 2 novembre 2022 du ministre de l'intérieur et des outre-mer relative à la sécurité des « villages-rugby » présente les principes directeurs de sécurité des « villages-rugby » organisés par les 9 villes hôtes, des autres sites de célébration (retransmission publique des matchs dans les « live-sites ») et des « festivals rugby » ;
- L'instruction (NOR : IOMK2232990J) du 25 novembre 2022 des ministres de l'intérieur et des sports relative à la sécurité de la coupe du monde de rugby et à l'organisation des grands événements internationaux définit les principes d'action pour la sécurité de la CMR ainsi que la répartition des compétences entre l'Etat et l'organisateur.

- les mesures qui en découlent pour le contrôle des flux de personnes, de marchandises et de véhicules, le contrôle des sacs à l'entrée des établissements à chaque fois que cela est possible et le contrôle des accès aux différents sites et emprises bâtimentaires, la surveillance active aux abords des établissements ;
- la participation aux réunions d'état-major de sécurité et la communication aux partenaires des plans des bâtiments (plans de masse) actualisés ;
- l'élaboration et/ou la mise à jour des dispositifs de gestion de crise ;
- la participation des établissements aux formations et sensibilisations aux enjeux de sûreté et à la gestion de crise.

3. Mesures numériques actives activés sur avis de l'ANSSI

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 préconisé de consulter régulièrement les sites suivants : https://www.ssi.gouv.fr (site de l'Agence nationale de la sécurité des systèmes d'information) et https://www.cert.ssi.gouv.fr (site du centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques).

- Mesure NUM 11-02 : rechercher sur le SI des marqueurs particuliers correspondant à une attaque
- Mesure NUM 21-02 : consulter régulièrement les sources d'information relatives aux vulnérabilités et attaques (site Internet du CERT-FR)
- Mesure NUM 31-03 : absorber le trafic illégitime au niveau du réseau
- Mesure NUM 31.06 : sensibiliser les utilisateurs sur un risque de sécurité et un comportement à adopter
- Mesure NUM 41.01 : valider et appliquer un correctif de sécurité
- Mesure NUM 51-01 : vérifier les annuaires de crise et le fonctionnement des moyens de communication sécurisés
- Mesure NUM 51-06 : procéder régulièrement à un séquestre hors ligne exceptionnel des sauvegardes des systèmes les plus critiques

Le fonctionnaire de sécurité des systèmes d'information confirme les mesures précédemment relayées[4].

[4] - 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. Le service SILENE de l'ANSSI, auquel ont accès les RSSI, permet une meilleure connaissance de l'exposition aux menaces de tout établissement ;
- Mener des actions de renforcement de la sécurité des annuaires électroniques afin de réduire les risques de diffusion de rançongiciels. Le service ADS de l'ANSSI, auquel ont accès les RSSI, permet de disposer d'un état des lieux de la sécurité des annuaires électroniques et de plans d'actions de renforcement ;
- S'assurer de la complétude des politiques de sauvegardes informatiques et des capacités à disposer de sauvegardes déconnectées résistantes aux rançongiciels ;
- 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 aux menaces cyber et aux bonnes pratiques à adopter au quotidien, en particulier sur les menaces d'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 ;
- Signaler systématiquement les incidents significatifs de sécurité numérique au 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. Ces signalements ont notamment permis de coordonner la réponse ministérielle lors de la vague de messages menaçants à caractère terroriste, transmis via des moyens numériques variés.

Annexe 3 : synthèse des mesures antérieures maintenues à l'été e l'automne 2023 »

1. Sécurité des lieux de rassemblement

Préalablement à l'organisation de tout événement, les responsables et initiateurs doivent prendre contact avec les FSI et les services préfectoraux même si 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[5] qui leur incombent en fonction des vulnérabilités particulières des lieux, de la fréquentation et des amplitudes horaires d'ouverture (jour/nuit), du contexte local évalué avec les services de l'État. Les personnels de l'équipe d'organisation seront sensibilisés aux bons comportements à adopter en cas de situation suspecte, de menace d'attaque terroriste, de confinement ou d'évacuation selon les situations.

Le ministère de l'intérieur a publié en 2018 un guide des bonnes pratiques de sécurisation d'un événement de voie publique[6].

2. Sécurité des grands espaces de tourisme et de loisirs, des sites touristiques, culturels et des transports collectifs

Chacun de ces sites reste une cible privilégiée notamment au moment des pics de fréquentation pendant les vacances scolaires et fait l'objet d'une vigilance renforcée. En cas de menace d'événement, les responsables de sûreté des établissements sont informés afin d'adapter leur dispositif.

3. Protection des ressortissants et des intérêts français à l'étranger

Il convient, pour tout voyage/mission à l'étranger dans le cadre de l'activité des établissements et personnels relevant des établissements des périmètres ministériels, de :

- Se référer aux « Conseils aux voyageurs » ou « Voyager en Europe »
- S'inscrire sur Ariane ainsi que sur le registre des Français à l'étranger sur le site du consulat s'agissant des ressortissants français qui s'installent plus de six mois à l'étranger.

4. Sécurité des bâtiments publics

Un effort particulier devra être porté sur la protection des sites des services de l'Etat. Il convient d'actualiser les annuaires partagés de crise et les procédures d'alerte afférentes. De même, les plans de protection et les procédures internes d'évacuation ou de confinement seront portés à la connaissance des nouveaux arrivants.

5. Sensibilisation à la menace des attaques par véhicules-béliers

Les organisateurs d'événements de voie publique doivent prendre en compte cette menace et mettre en œuvre des dispositifs de protection adaptés, après avis des référents sûreté locaux et/ou consultation de la fiche de recommandations Vigipirate « Se protéger contre les attaques au véhicule-bélier », disponible sur le site Internet du SGDSN et du guide des bonnes pratiques de sécurisation d'un événement de voie publique.

[5] https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Securisation-des-evenements-de-voie-publique
[6] https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenements-de-voie-publique

6. Vigilance et mesures de prévention face au risque NRBC-E (nucléaire, radiologique, biologique, chimique, explosif)[7]

Au moindre doute sur le contenu d'un colis ou d'une enveloppe, il ne faut pas les manipuler, mais alerter les forces de sécurité intérieure (appel au 17 ou 112) et établir un périmètre de sécurité en faisant évacuer et en balisant la zone.

Par ailleurs, tout vol, disparition de substance NRBC doit être signalé 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).

7. Sensibilisation à la lutte anti-drone

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.

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

Le signalement des cas suspects de radicalisation, quel que soit le type de radicalisation (religieuse, politique…) s'effectue 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.

Des actions de sensibilisation sont conduites au sein de la fonction publique[8]. Un référent radicalisation/sécurité en préfecture a vocation à servir d'interlocuteur local pour cette problématique.

9. Communication du niveau VIGIPIRATE

Vous veillerez à mettre en place les logogrammes : « **Sécurité renforcée - risque attentat** ».

Ces logogrammes peuvent être téléchargés sur les sites du Gouvernement.

10. Sensibilisation du grand public aux bonnes pratiques

Un ensemble de guides de bonnes pratiques à destination des professionnels et des particuliers sont accessibles en ligne sur le site du SGDSN et sur l'espace dédié du site du Gouvernement.

Des documents sont également disponibles sur le site du SGDSN :

- La version publique du **plan Vigipirate « Faire Face Ensemble »**, également disponible en langue anglaise
- Des affiches à l'onglet « affiches de sensibilisation »
- Un ensemble de guides et de fiches de recommandations et de bonnes pratiques à l'attention du grand public est également téléchargeable sur le site du SGDSN
- Une **plateforme de sensibilisation VIGIPIRATE,** outil ludique et accessible par tous qui permet d'être sensibilisé à la menace terroriste et d'avoir une meilleure connaissance des gestes et réflexes à adopter,

[7] En Espagne, à la fin du mois de novembre 2022, une recrudescence d'envois de lettres ou de colis piégés a été constatée.

[8] https://www.fonction-publique.gouv.fr/files/files/Publications/Coll%20outils%20de%20la%20GRH/guide-prevention-radicalisation.pdf