PRÉFET
DES ALPES-
MARITIMES

Liberté
Égalité
Fraternité

Cabinet - Direction des sécurités
Service interministériel de défense et de protection civiles

VIGIPIRATE
URGENCE ATTENTAT

Nice, le 03 JUIL. 2025

Le préfet des Alpes-Maritimes

à

Mesdames et messieurs les maires

Monsieur le président du conseil régional

Monsieur le président du conseil départemental
Mesdames et messieurs les présidents d'établissements
de coopération intercommunale

Objet : Adaptation de la posture VIGIPIRATE **"été - automne 2025"**.
Maintien au niveau « Urgence Attentat ».

Réf. : Plan gouvernemental VIGIPIRATE du 1er décembre 2016 (édition mai 2019).

La posture Vigipirate **"été - automne 2025",** applicable dès à présent et jusqu'à nouvel ordre, maintient l'ensemble du territoire national au niveau le plus élevé **"urgence attentat",** au regard de l'état de la menace terroriste et de l'instabilité au Proche et Moyen-Orient.

Cette posture met l'accent sur :

- la sécurité des lieux de culte et des établissements d'enseignements ;
- la sécurité des rassemblements festifs, culturels et religieux ;
- la sécurité des bâtiments publics et institutionnels ainsi que des transports ;
- la sécurité du numérique.

1. Sécurité des lieux de rassemblement et des lieux de culte

a) Lieux de rassemblement

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.

Une vigilance accrue, quant à la détention d'armes blanches ou autres objets suspects, sera portée lors des contrôles mis en place aux différents accès de ces rassemblements.

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. 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.

Une vigilance particulière sera notamment portée lors des rassemblements liés aux événements suivants :

- Soldes d'été du **26 juin au 23 juillet 2025** ;
- 90ème anniversaire de la mort d'Alfred Dreyfus le **12 juillet 2025** ;
- Fête nationale le **14 juillet 2025 ;**
- 9ème commémoration de l'attentat de Nice le **14 juillet 2025 ;**
- 80ème anniversaire du procès du maréchal Pétain du **23 juillet au 15 août 2025 ;**
- Nice Jazz Festival du **24 au 27 juillet 2025 ;**
- 30ème anniversaire d'une vague d'attentats en France, attribués au Groupe islamique armé le **25 juillet 2025 ;**
- Rentrée scolaire le **1er septembre 2025 ;**
- *International Congress on Advances in Nuclear Power Plants* à Antibes du **17 au 19 septembre 2025** ;
- 42ème édition des Journées européennes du patrimoine les **20 et 21 septembre 2025** ;
- 2ème anniversaire de l'attaque du Hamas contre Israël le **7 octobre 2025** ;
- Première édition européenne de l'Evo (e-game) à Nice le **10 octobre 2025** ;
- 5ème anniversaire de l'assassinat de Samuel Paty le **16 octobre 2025** ;
- Vacances de la Toussaint du **18 octobre au 3 novembre 2025** ;

- Commémoration du 11 novembre 1918 le **11 novembre 2025** ;
- 10ème anniversaire des attentats du 13 novembre 2015 le **13 novembre 2025 ;**
- Marchés de Noël du **25 novembre au 25 décembre 2025** ;
- Téléthon les **5 et 6 décembre 2025** ;
- Commémoration de l'attentat du marché de Noël de Strasbourg en 2018 le **11 décembre 2025** ;
- Vacances de Noël du **20 décembre au 5 janvier 2025** ;
- Coupe d'Afrique des Nations de football (organisée au Maroc) du **21 décembre au 18 janvier 2025** ;
- Saint-Sylvestre le **31 décembre 2025**.

b) Mesures propres aux fêtes religieuses se déroulant tout au long de l'année, quel que soit le culte concerné (mais plus particulièrement les cultes chrétien, juif et musulman).

Lors des fêtes religieuses, la sécurité restera 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 ou très sensibles par les autorités religieuses.

La sécurité devra être plus particulièrement renforcée lors des fêtes religieuses suivantes :

- Achoura (fête chiite) le **6 juillet 2025** ;
- Tisha Beav (fête juive) les **2 et 3 août 2025 ;**
- Assomption (fête chrétienne) le **15 août 2025 ;**
- Al-Mawlid (fête musulmane) les **4 et 5 septembre 2025** ;
- Roch Hachana (fête juive) les **23 et 24 septembre 2025** ;
- Yom Kippour (fête juive) le **2 octobre 2025** ;
- Souccot (fête juive) du **6 au 15 octobre 2025** ;
- Toussaint (fête chrétienne) le **1er novembre 2025** ;
- Hanouka (fête juive) du **14 au 22 décembre 2025** ;
- Veillée de Noël (fête chrétienne) le **24 décembre 2025** ;
- Noël (fête chrétienne) le **25 décembre 2025**.

Je vous demande, lors de ces événements, de mobiliser vos moyens de vidéoprotection ainsi que vos policiers municipaux lorsque vous en disposez. 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 fortement recommandée.

Une attention particulière devra être portée aux véhicules en stationnement à proximité des lieux de rassemblement ou du culte. À cet égard, vous pourrez, si nécessaire prendre des mesures temporaires d'interdiction de circuler et de stationner. La contribution des polices municipales à la sécurisation des lieux de rassemblement et de culte se fera en coordination avec les forces étatiques.

c) Mesures propres aux périodes de vacances scolaires

Les lieux sujets à de fortes affluences saisonnières durant les vacances scolaires (stations balnéaires, salles de spectacles, etc.) bénéficieront de moyens adaptés. Les services de l'État (forces de sécurité intérieure et unités Sentinelle) adapteront leur dispositif en conséquence.

J'invite les opérateurs à solliciter l'appui des référents sûreté départementaux de la police ou de la gendarmerie nationales.

Je vous demande de porter une attention particulière sur la sécurisation des transports collectifs de personnes, particulièrement fréquentés lors des périodes des congés scolaires : plateformes aéroportuaires, gares, ports et réseaux de transport en commun.

d) Guide des bonnes pratiques de sécurisation d'un événement de voie publique

Le ministère de l'Intérieur a publié et diffusé un "Guide des bonnes pratiques de sécurisation d'un événement de voie publique" en octobre 2018. Il est disponible sur le site Internet du ministère de l'Intérieur :

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

Il peut être utilement complété du guide des bonnes pratiques pour la sûreté des espaces publics accessible via le lien https://www.sgdsn.gouv.fr/vigipirate/les-guides.

2. 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.

Je vous demande d'appliquer de manière rigoureuse les mesures Vigipirate, et de signaler aux autorités compétentes toute menace ou tout incident pouvant s'apparenter à une attaque terroriste.

a) Sites touristiques et de loisirs

Compte tenu de la situation internationale et de la persistance de la menace, les mesures de vigilance doivent être renforcées par les acteurs des secteurs du tourisme et des loisirs (exploitants de parcs de loisirs, de salles de spectacles, de plages, etc).

Les lieux très fréquentés, à l'instar des stations balnéaires, bénéficieront des moyens des services de l'État (forces de sécurité intérieure et unités Sentinelle) qui adapteront leur dispositif en conséquence.

Les polices municipales demeurent également mobilisées.

b) Espaces de commerce

La sécurité doit rester renforcée autour des grands espaces de rassemblements ayant pour objet des activités commerciales (salons, expositions, foires, etc.), et les interconnexions de transports en milieu clos (gares, aéroports, etc.) dotées de commerces.

La sécurité autour des grands espaces de commerce, notamment lors des soldes d'hiver qui provoquent une forte affluence, demeure un axe d'attention majeur.

La sécurisation de ces grands espaces passe entre autres par :

- La sensibilisation des personnels : elle doit être assurée par les gestionnaires de centres et d'enseignes commerciaux ;
- Le renforcement des échanges et de la coordination entre acteurs publics et privés : mise en place de conventions locales de coopération avec les forces de sécurité ;
- 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.

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 la mesure du possible, je pourrais accorder l'extension de cette vidéosurveillance aux abords immédiats de la voie publique et aux espaces de commerce.

De même, je pourrais autoriser, à titre exceptionnel, la présence d'agents privés de sécurité, même itinérants, sur la voie publique, aux abords des sites des espaces de commerce qui en feront la demande.

3. 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.). À ces occasions, le niveau de sécurité des plateformes aéroportuaires, des gares, des ports et des réseaux de transport en commun doit être renforcé. Une vigilance particulière sera également portée dans les transports lors des vacances scolaires.

a) Espaces d'accueil des voyageurs pour tout mode de transport

La menace visant les emprises des gares, des aérogares et des stations de métro ou de RER impose une vigilance quotidienne. Les couloirs de liaison intermodaux doivent faire l'objet d'une attention particulière.

b) Spécificité du transport aérien

Les gestionnaires d'aéroports et les compagnies aériennes maintiendront leur haut niveau de vigilance lors des contrôles d'embarquement des passagers. Les services de l'État et les opérateurs poursuivront l'amélioration de la sécurisation du côté ville.

Une coordination étroite entre les forces de sécurité intérieure (FSI), les armées et les opérateurs doit permettre une intervention rapide. La communication envers des passagers ne maîtrisant pas la langue française doit être prise en compte.

c) Infrastructures et réseaux ferroviaires

Les transports terrestres constituent toujours une cible d'intérêt, à la symbolique et l'impact forts.

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 ;
- courriel : permanence.cmvoa@developpement-durable.gouv.fr

4. Sécurité du transport maritime de passagers

Il est demandé aux exploitants portuaires et aux armateurs d'assurer la continuité du contrôle des véhicules, de leurs passagers et de leur chargement. Je vous rappelle que tout armateur exploitant des navires rouliers à passagers doit mettre en place un dispositif destiné à prévenir l'introduction des articles prohibés (armes à feu, explosifs, etc.) par les personnes en sortie des espaces rouliers, au moment de leur accès aux espaces publics du navire.

Je vous demande également un effort de ciblage, reposant sur l'analyse et la détection de comportements particuliers avant l'embarquement, en liaison avec les autorités portuaires (enregistrement tardif, véhicule de location, personne seule dans le véhicule, etc.).

5. Sécurité des bâtiments publics

Les installations et bâtiments publics tels que les sites institutionnels constituent des cibles potentielles. Je vous demande donc de prendre toutes les mesures de vigilance nécessaires, particulièrement aux abords des accueils du public (sites préfectoraux et/ou interministériels situés hors du siège de la préfecture, centres administratifs, mairies,..etc..).

6. Sécurité des établissements d'enseignement et de recherche

L'adaptation de cette posture met l'accent sur :

- Le maintien des efforts en matière de sécurité des établissements et de protection des personnes ;

- le maintien d'une haute vigilance quant à la sécurisation des systèmes d'information, notamment face à la récente vague d'incidents de sécurité numérique et au vu de l'évaluation de la menace cyber.

a) Information et coordination entre les acteurs

Des échanges doivent être engagés, maintenus et renforcés avec les partenaires locaux, notamment les correspondants en préfecture et auprès des instances dédiées, afin que soient identifiés les établissements, activités ou zones les plus à risque. L'état de la menace devra être connu et partagé entre les acteurs. Toute menace, violence ou atteinte à la sécurité devra être signalée aux autorités et partenaires concernés.

b) Mesures de sécurisation des personnes et des biens

Les établissements d'enseignement et de recherche sont des cibles privilégiées.

Une attention particulière doit être 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.

La posture "été – automne 2025" active la mesure IMD 12-03 qui vise à protéger les lieux de production et de stockage des matières dangereuses et leurs transports.

c) Sécurité des systèmes d'information

Le maintien d'une vigilance quant à la sécurité des systèmes d'information est de rigueur en s'appuyant sur tous les acteurs ministériels et les consignes relayées par le fonctionnaire de sécurité des systèmes d'information.

7. Sécurité des sites culturels

Les établissements culturels sont susceptibles de constituer des cibles privilégiées, d'individus poursuivant des finalités revendicatives ou pire, terroristes. Aussi, dans le contexte sécuritaire actuel marqué par les bouleversements affectant la zone moyen-orientale et leurs éventuelles répercussions sur le territoire national, je vous demande d'être vigilant dans le secteur culturel, en vue d'assurer une protection adéquate de ces établissements, mais aussi une sécurité efficace des évènements qui y seront programmés.

Dans ces conditions, il importe que vous poursuiviez le déploiement de mesures de sécurité renforcées, telles qu'une surveillance accrue et des contrôles de sécurité rigoureux aux accès de vos sites, y compris si ceux-ci accueillent une population restreinte. Le filtrage et la fouille visuelle des sacs revêt une importance accrue au regard de la menace endogène signalée par les services, notamment en raison de la jeunesse de cette menace très perméable aux discours diffusés sur les réseaux sociaux.

Ces mesures viseront à dissuader toute tentative d'attaque terroriste et à garantir un environnement plus sûr.

8. Sécurité des opérateurs relevant des ministères sociaux

Les formes de la menace terroriste se diversifient et se traduisent par des actions violentes et spectaculaires.

Les organismes des ministères sociaux, représentant l'action de l'État au profit de ses ressortissants, sont des cibles à la fois symboliques, et vulnérables du fait de leur vocation d'accueil du public. Une extrême vigilance est donc requise.

Les opérateurs veilleront par conséquent à disposer de plans de sûreté à jour, à mettre en œuvre les mesures Vigipirate qui les concernent, en coordination étroite y compris lors des planifications et exercices, avec leurs partenaires locaux (préfecture, forces de sécurité intérieure, services d'incendie et de secours, *etc.*).

Cette vigilance dans les champs matériels concerne tout autant les champs immatériels : les systèmes d'information sont des cibles régulières d'attaques du fait de leurs vulnérabilités.

Aussi, je vous demande :

- d'avoir le souci constant d'informer sans délai et avec précision les autorités (chaîne ministérielle et chaîne préfectorale) de tous signaux faibles ou incidents pouvant s'apparenter à une préparation ou à une attaque terroriste ;
- de profiter de toute occasion pour sensibiliser et entraîner le personnel à la détection des signaux faibles en les appelant à la plus grande vigilance dans l'exercice de leur fonction.

a) Secteurs santé et solidarités

Je souhaite le maintien des actions mises en œuvre par les forces de sécurité intérieure, notamment la sécurisation des abords des *opérateurs d'importance vitale* (OIV) et des établissements de santé de niveau 1, selon la cartographie transmise par les *agences régionales de santé* (ARS). Elles veilleront, en cas d'attentat, au renforcement immédiat des établissements accueillant des victimes, ainsi qu'à la protection des forces de secours intervenant *in situ*.

b) Secteurs social et travail

Les agences et opérateurs chargés de la mise en œuvre locale des politiques de l'emploi restent des cibles hautement symboliques pour des individus souhaitant attaquer l'État. Ces derniers pourraient ainsi saisir toute occasion pouvant servir leurs objectifs pour diffuser et amplifier leurs revendications au moyen de contestations, toujours spectaculaires et éventuellement violentes, dans les lieux accueillant du public.

En conséquence, je vous demande de mettre en œuvre les mesures de sûreté demandées par la posture Vigipirate, et notamment toutes celles liées à la protection des bâtiments et des installations. Vous pourrez vous aider de la documentation disponible aux adresses suivantes :

- https://sante.gouv.fr/ministere/defense-et-securite-hfds/les-guides-du-hfds
- https://www.sgdsn.gouv.fr/files/files/Publications/guide-unique-de-sensibilation-vigipirate-pact-num-v7.pdf (guide des bonnes pratiques pour la sureté des espaces publics).

9. Sécurité du numérique

Au regard de l'évaluation de la menace pour la sécurité du numérique, il apparaît nécessaire de **vérifier les annuaires de crise régulièrement, et le bon fonctionnement des moyens de communication sécurisés.**

Les objectifs et mesures de sécurité suivants doivent être appliqués :

- **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'information. 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 système d'information et les technologies le composant afin de pouvoir agir en cas de vulnérabilité et/ou de fin de support d'une solution informatique.

L'ANSSI propose en ce sens un guide permettant de mettre en place un processus de cartographie des SI (https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation).

- **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.

- **créer des alertes de sécurité en analysant les journaux ou en activant des paramètres de supervision ;**
- **consulter régulièrement les sources d'information relatives aux vulnérabilités et attaques** (site Internet du CERT-FR)

Afin de se prémunir d'éventuelles attaques, il convient de mettre en place un processus de veille (quotidienne) concernant la publication de vulnérabilités concernant les éléments du système d'information. 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/).

- **absorber le trafic illégitime au niveau du réseau**

Il est important de s'assurer que les opérateurs de services numériques disposent d'infrastructures et composants de sécurité permettant d'absorber le trafic, qu'ils puissent transmettre à leurs clients une liste d'adresses IP illégitimes à bloquer, et 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. Les organisations doivent ensuite 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.

- **sensibiliser les utilisateurs sur un risque de sécurité et un comportement à adopter**

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

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

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 portent sur 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.

- **valider et appliquer un correctif de sécurité**

Face aux vulnérabilités critiques 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 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 correspondant 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://www.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-2024-ALE-013, CERTFR-2024-ALE-011, CERTFR-2024-ALE-008, CERTFR-2024-ALE-007, CERTFR-2024-ALE-006, CERTFR-2024-ALE-004, CERTFR-2024-ALE-001, CERTFR-2023-ALE-012, CERTFR-2023-ALE-008, CERTFR-2023-ALE-004, CERTFR-2022-ALE-013 du CERT-FR)

De nombreux équipements comme les pare feux et les passerelles VPN sont régulièrement la cible des attaquants qui continuent de trouver des vulnérabilités leur permettant de les compromettre pour prendre pied dans le système d'information ou d'obtenir des secrets d'authentification pour usurper l'identité des utilisateurs. Les vulnérabilités sur les produits de l'éditeur IVANTI (CERT-2024-ALE-001) ont ainsi été et continuent d'être activement exploitées par un acteur de la menace réputé chinois. Plus récemment encore, les solutions Palo Alto Networks GlobalProtect (CERTFR-2024-ALE-006) ou encore FortiOS (CERTFR-2024-ALE-004) ont eux aussi fait l'objet d'exploitations ciblées puis massives.

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.

Ces exemples démontrent l'importance d'une bonne connaissance de ses systèmes d'information et de la présence d'un processus de veille et de gestion des vulnérabilités pour mieux les anticiper ou réagir rapidement. Cela est d'autant plus important qu'il peut être délicat de mettre à jour des équipements et installer des correctifs, des incompatibilités pouvant parfois émerger et rendre indisponibles des services.

➔ **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. Les utilisateurs de ces systèmes doivent vérifier la nécessité de maintenir une accessibilité de ces équipements à distance et, si cela s'avère être 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).

- **vérifier les annuaires de crise et le fonctionnement des moyens de communication sécurisés ;**
- **adapter les dispositifs de réponse à incidents aux caractéristiques de la menace**

Afin de s'assurer d'être en mesure de répondre de manière rapide et efficace 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, les organisations doivent également vérifier qu'un *plan de continuité d'activité* (PCA), détaillant les besoins de continuité de leur centre opérationnel, existe et puisse être mobilisé pour assurer la continuité de la réponse en cas d'incident, même de nature non-cyber (dysfonctionnement électrique, télécoms, indisponibilité bâtimentaire, *etc.*). Les moyens de continuité identifiés via le PCA doivent être vérifiés via des tests et des exercices afin d'assurer de leur parfaite disponibilité et efficacité en cas d'incident les mobilisant.

- **réaliser des tests de restauration des sauvegardes**

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 des politiques de sauvegarde et de la réalisation des tests : https://cyber.gouv.fr/publications/guide-dhygiene-informatique.

- **procéder régulièrement à un séquestre hors ligne exceptionnel des sauvegardes des systèmes les plus critiques.**

10. Consignes particulières

1.1. Sensibilisation du personnel en tenue

Toutes les personnes, civiles ou militaires, portant un uniforme ou une tenue avec des signes distinctifs, et représentant une autorité, restent des cibles privilégiées. Elles seront sensibilisées et informées par leurs autorités de tutelle des mesures de sécurité à appliquer.

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

Les attaques par véhicules-béliers demeurent un mode d'action privilégié des 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 : https://www.sgdsn.gouv.fr/files/files/Publications/fiche-se-proteger-contre-les-attaques-au-vehicule-belier.pdf
- le guide du ministère de l'Intérieur accessible via le lien suivant : https://www.interieur.gouv.fr/Publications/Securite-interieure/Securisation-des-evenements-de-voie-publique

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

La radicalisation se caractérise par un changement de comportement qui peut conduire certaines personnes à l'extrémisme ou au terrorisme. Des troubles psychologiques peuvent offrir un terreau favorable à la radicalisation. L'objectif du signalement au *centre national d'assistance et de prévention de la radicalisation* (CNAPR) est de protéger ces personnes contre elles-mêmes et la population contre de possibles comportements violents. Les combinaisons de comportements suivants doivent éveiller la vigilance et méritent de faire l'objet d'un signalement : changements physiques, vestimentaires et alimentaires, propos asociaux, passage à une pratique religieuse hyper ritualisée, rejet de l'autorité, repli sur soi, rejet brutal des habitudes quotidiennes, refus du débat, rejet de la société et des institutions, modification soudaine des centres d'intérêt, discours complotiste ou apocalyptique, tentative d'imposition agressive d'un ordre religieux.

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

➔ **Appel au numéro vert : 0 800 005 696**

En cas de suspicion d'une action violente ou de tout autre cas d'urgence, appeler immédiatement le 17 ou le 112 pour alerter les forces de sécurité intérieure.

Des actions de sensibilisation sont conduites au sein de la fonction publique (https://www.fonction-publique.gouv.fr/files/files/publications/publications-dgafp/guide-prevention-radicalisation.pdf). Je vous rappelle qu'il existe au sein de mes services des référents radicalisation/sécurité qui sont vos interlocuteurs locaux pour cette problématique.

Chaque événement terroriste donne lieu à des conseils de vigilance particuliers, adaptés à l'évolution de la menace, ainsi qu'à des consignes précises, notamment au sein des *groupes d'évaluation départementaux* (GED) de la radicalisation islamiste, sous la responsabilité du Ministère de l'Intérieur.

1.4. Vigilance et mesures de prévention face à la menace NRBC-E (nucléaire, radiologique, biologique, chimique, explosif)

Les récents attentats ou actes de malveillance commis ou déjoués en Europe ont démontré une capacité à fabriquer des explosifs artisanaux ou des substances toxiques à partir de produits chimiques d'usage courant.

a) Cas particuliers des colis ou plis suspects

Au moindre doute sur le contenu d'un colis ou d'une enveloppe, ce dernier ne doit pas être manipulé. Il doit être contrôlé au moyen d'un détecteur à rayons X. En cas d'impossibilité à mettre en œuvre ce type de technologie, il convient d'alerter les forces de sécurité intérieure (appel au 17 ou au 112) et d'établir un périmètre de sécurité en faisant évacuer et en balisant la zone. Dans le cas où un pli contenant une poudre a été ouvert et que des personnes ont été en contact avec le produit, il convient également d'alerter les services de secours (18 ou 112) et d'isoler les personnes ayant été en contact dans une pièce attenante, en leur demandant de ne pas manger, boire ou fumer dans l'attente de l'arrivée des secours.

b) Signalement des transactions suspectes

Les professionnels qui vendent des explosifs artisanaux ou des substances NRBC 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. Le contact se fait de la manière suivante :

Mail à pixaf@gendarmerie.interieur.gouv.fr / Appel au 01 78 47 34 96 (24/7)

1.5. Lutte anti-drones

L'utilisation détournée de drones peut permettre de perpétrer des actes de malveillance ou à caractère terroriste.

Les responsables d'activités sensibles et de grands rassemblements doivent prendre en compte cette menace en menant une analyse de risques avec l'appui des référents de sûreté locaux de la police ou de la gendarmerie nationales.

L'installation de moyens de détection des drones aux abords de leur site, permettent la mise en œuvre des mesures de sauvegarde immédiate en cas de menace imminente, l'orientation des forces de sécurité vers le télé-pilote pour mettre fin au survol, et le relevé des éléments de preuve des infractions.

Par arrêté, je pourrais interdire l'usage et/ou le transport des drones dans un temps et un périmètre déterminés.

Les événements les plus sensibles peuvent également donner lieu, en fonction de l'évaluation de la menace et sur décision du Premier Ministre, au déploiement d'un *dispositif particulier de sûreté aérienne* (DPSA) placé sous le commandement du *commandant de la défense aérienne et des opérations aériennes* (CDAOA) et incluant des moyens de lutte anti-drones.

La posture "été – automne 2025" active la mesure ALR 11-05 qui vise à interdire l'usage et/ou le transport de drones dans les périmètres déterminés par les autorités préfectorales.

11. Information du grand public

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

a) Efforts de communication

Si ce n'est pas déjà le cas, vous devez mettre en place le logogramme : ***"urgence attentat".***

Ce logogramme peut être téléchargé sur le site du SGDSN à partir du lien suivant : https://www.sgdsn.gouv.fr/files/files/Vigipirate/logogrammes-vigipirate.pdf

b) Promotion des 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".

Je vous demande de renforcer la communication des mesures et des comportements à adopter en cas d'attaque terroriste au sein des établissements et lieux recevant du public. Ces affiches peuvent être téléchargées, et imprimées sur un format adapté au lieu où elles sont placées, afin de les rendre visibles du public (privilégier les entrées et sorties des établissements, les halls 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-recommandations-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.

c) À destination des élus et des professionnels

En complément, plusieurs guides de bonnes pratiques, 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.

Enfin, deux modules de formation en ligne, développés en liaison avec plusieurs 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.

Au regard de l'état de la menace terroriste, de la guerre en Ukraine et de l'instabilité de la situation au Proche et Moyen-Orient, je demande à chacun de redoubler de vigilance. Il en va de la sécurité de nos concitoyens.

En cas d'attaque ou d'évolution significative de la menace terroriste, cette posture Vigipirate est susceptible de faire l'objet d'une adaptation, en urgence, en liaison avec le ministère de l'Intérieur et les services.

Le Préfet des Alpes-Maritimes

CAB 4942

Laurent HOTTIAUX