PRÉFET
DU PAS-DE-CALAIS
Liberté
Égalité
Fraternité

Direction des sécurités

Service interministériel de défense et protection civiles
Pôle Sûreté-Défense

Affaire suivie par Camille VASSEUR
pref-vigipirate62@pas-de-calais.gouv.fr

Arras, le 07 JUIL. 2026

REÇU
MAIRIE
08 JUIL. 2026
BILLY MONTIGNY
N° 2763

Le préfet du Pas-de-Calais

à

Mesdames et Messieurs les maires

Monsieur le président de l'AMF 62

Mesdames et Messieurs les présidents des EPCI

Monsieur le Président du conseil départemental

En communication à Mesdames et Messieurs les Sous-préfets d'arrondissement

OBJET : VIGIPIRATE – évolution du plan VIGIPIRATE et adaptation à la posture été - automne 2026 ».

Afin de s'adapter à l'évolution de la menace sur le territoire national, le plan VIGIPIRATE a connu une évolution depuis le 22 juin dernier. Désormais, il repose sur 3 stades d'alerte :

- « vigilance » : qui correspond au niveau d'alerte initial ;
- « vigilance renforcée » : qui correspond au niveau d'alerte intermédiaire ;
- « alerte attentat » : qui correspond au niveau d'alerte le plus élevé. Celui-ci peut être activé pendant 12 jours renouvelables sur décision expresse du Premier ministre.

La nouvelle posture du plan VIGIPIRATE « été - automne 2026 » est également applicable à compter du 22 juin 2026. L'ensemble du territoire national est désormais placé en ***« vigilance renforcée ».***
La nouvelle posture met l'accent sur :
- la lutte contre la menace drones ;
- la sécurité des sites touristiques et les zones d'affluences lors des vacances d'été et de Noël 2026 ;
- la sécurité des bâtiments publics et institutionnels.

Les vulnérabilités d'ordre général de l'activité clé « sécurisation » identifiées sur la période « été-automne 2026 » sont les suivantes :

- • maintien d'une menace terroriste élevée avec risque d'actions isolées et difficilement détectables ;
- concentration saisonnière de population dans les zones touristiques littorales et montagneuses ;
- multiplication des grands événements culturels, festifs, sportifs et commémoratifs durant la période estivale entraînant une forte sollicitation des forces de sécurité intérieure et de fortes concentrations de population ;
- exposition persistante des élus à des actions violentes ou de contestation radicalisée ;
- tension sur les effectifs disponibles en raison des permissions estivales.

Je vous informe que les militaires de la force sentinelle pourront toujours venir en appui des forces de sécurité intérieure pour la sécurisation des évènements et des lieux de culte, selon une programmation trimestrielle, issue d'un dialogue civilo-militaire.

1. Concernant les établissements et manifestations culturelles :

La période estivale et le début de l'automne 2026 présentent un niveau de sensibilité en raison de l'intensification des flux touristiques, de la multiplication des festivals, concerts et spectacles en plein air, ainsi que de l'augmentation de la fréquentation des grands sites patrimoniaux et culturels. Cette concentration d'activités et de publics accroît l'exposition des lieux culturels à la menace terroriste, notamment à des actions visant les rassemblements à forte visibilité et densité de fréquentation.

Les vulnérabilités concernent principalement les espaces ouverts ou semi-ouverts accueillant un public nombreux, les accès principaux et secondaires, les zones d'attente et de circulation, les abords immédiats des établissements ainsi que les accès logistiques et techniques liés aux phases de montage, démontage et livraison. Le recours accru à des personnels saisonniers ou prestataires temporaires peut également fragiliser l'application homogène des procédures de sûreté.

1.1. Les objectifs :

La contribution des polices municipales à la sécurisation des lieux de rassemblement est essentielle, en toute coordination avec les forces étatiques, afin de :

- garantir une posture visible, réactive et dissuasive des FSI sur le territoire ;
- assurer la protection des personnes et des biens sur le territoire ;
- maintenir la continuité de la présence territoriale en période estivale ;
- adapter la posture des FSI aux mouvements de population ;
- garantir la capacité de montée en puissance rapide des dispositifs de sécurisation et d'intervention.

1.2. Consignes particulières :

Les consignes particulières de l'activité clé « sécurisation », sur la période « été-automne 2026 », sont les suivants :

- augmenter la présence des militaires de la gendarmerie et des forces de police dans les zones de concentration des populations ;

- accentuer les contrôles des flux sur les axes les plus fréquentés ;
- porter une attention particulière à la menace drone et aux capacités de neutralisation associées ;
- assurer une remontée immédiate des événements significatifs.

Les établissements et organisateurs relevant du secteur culturel veilleront à adapter les dispositifs de filtrage et de contrôle d'accès aux niveaux de fréquentation attendus, notamment lors des événements de grande affluence ou organisés dans des espaces ouverts au public. Une vigilance particulière devra être portée aux accès secondaires, zones techniques, livraisons et phases de montage ou démontage.

Les mesures de protection physique des abords et des accès sensibles devront être systématiquement vérifiées avant l'ouverture des manifestations accueillant un public important. Les exploitants renforceront également la présence visible des personnels de sécurité aux périodes de forte fréquentation et s'assureront de la bonne diffusion des procédures d'alerte et de signalement auprès des personnels permanents, saisonniers et prestataires.

Enfin, une coordination régulière devra être maintenue avec les préfectures, forces de sécurité intérieure et services de secours afin de garantir l'adaptation des dispositifs au niveau de menace terroriste et aux spécificités propres de chaque événement ou établissement culturel.

2. Concernant le secteur d'activité « social et sociétal » :

2.1. Vulnérabilités

- Vulnérabilités d'ordre général :

Les vulnérabilités d'ordre général de l'activité clé « social et sociétal » identifiées sur la période « été-automne 2026 » sont les suivantes :

- persistance d'un climat de tensions sociales susceptible de générer des mobilisations violentes ;
- radicalisation de certains modes d'action adverse ;
- sensibilité particulière des sujets environnementaux et agricoles pouvant entraîner des mouvements localisés à forte intensité ;
- vulnérabilité accrue des élus locaux et représentants de l'État face aux phénomènes d'intimidation, violences ou pressions ;
- élections à fort enjeu politique et sociétal dans les Outre-Mer (Nouvelle-Calédonie) ;
- capacité de mobilisation rapide via réseaux sociaux ;
- risque d'instrumentalisation informationnelle d'événements sécuritaires ou sociétaux dans une logique de déstabilisation.

- Vulnérabilités des établissements d'enseignement et de recherche et structures d'accueil collectif de mineurs relevant de la tutelle des ministères chargés de l'éducation, de l'enseignement supérieur et de la recherche, de la culture et de l'agriculture :

- maintien de la menace contre les établissements et structures des périmètres de l'éducation nationale, y compris les établissements privés, de l'enseignement supérieur et de la recherche qui sont des cibles privilégiées ;
- émergence de nouvelles formes d'extrémisme violent ;
- rajeunissement des auteurs d'infractions terroristes ;
- importance du port de couteaux par les élèves.

2.2. Les objectifs :

Les objectifs de sécurité de l'activité clé « social et sociétal » à atteindre, sur la période « été-automne 2026 », sont les suivants :

- garantir la sécurité des élus, représentants de l'État, emprises publiques et symboles institutionnels ;
- préserver la capacité de réaction des FSI face à des mobilisations soudaines ou non déclarées ;
- maintenir une remontée fiable et rapide du renseignement territorial vers les échelons de conduite ;
- déceler les troubles à l'ordre public à venir sur les réseaux sociaux.

En ce qui concerne les établissements d'enseignement, les objectifs à atteindre sont les suivants :

- échanges avec les services du ministère de l'intérieur pour identifier les établissements, les plus à risque ;
- signalement aux autorités administratives et judiciaires compétentes de toute menace, violence ou atteinte à la sécurité ;
- partage et actualisation des procédures de veille, d'alerte et de gestion de crise avec les services de défense et de sécurité académique (SDSA), le fonctionnaires de sécurité et de défense des établissements d'enseignement supérieur et de recherche, les préfectures, les forces de sécurité intérieure, etc ;
- mise en œuvre des mesures de sécurité VIGIPIRATE diffusées par le service du haut fonctionnaire de défense et de sécurité ;
- renforcement de la protection et du contrôle des laboratoires sensibles soumis à une réglementation spécifique, ainsi qu'aux lieux de stockage de matières dangereuses et animaleries ;
- vigilance maximale sur les zones sensibles (zones à régime restrictif, zones sécurisées, zones d'accès restreint) et signalements systématiques ;
- pour l'enseignement agricole, sécurisation des personnes selon les instructions du MAASA. Les chefs des missions de défense et sécurité de zone auprès des directions régionales de l'alimentation, de l'agriculture et de la forêt (DRAAF), seront inclus dans les échanges par les SDSA ;
- dans les ACM, sensibilisation des encadrants et des mineurs. Les responsables pourront s'appuyer sur la documentation disponible3 et se rapprocheront des gestionnaires des établissements d'accueil, des mairies, des préfectures, ainsi que des services de sécurité et de secours pour garantir la sécurité des personnes et des biens.

2.3. Consignes particulières

Les consignes particulières de l'activité clé « social et sociétal », sur la période « été-automne 2026 », sont les suivants :

- renforcer la veille des mouvements sociaux susceptibles d'affecter le TN ;
- identifier les événements à risque de débordement ou de récupération par des mouvances radicales ;
- porter une attention particulière aux atteintes visant les élus, bâtiments publics, forces de sécurité et infrastructures sensibles ;
- anticiper les besoins en forces mobiles ou de réserve opérationnelle ;
- préserver une posture de contact avec les élus et organisateurs afin d'éviter les effets de surprise ;
- intégrer le risque informationnel : rumeurs, appels viraux, désinformation ou instrumentalisation d'incidents.

3. Concernant les transports :

- ***Espaces d'accueil des voyageurs pour tout mode de transport***

La menace visant les emprises des gares et des aérogares impose une vigilance quotidienne. De même, les couloirs de liaison intermodaux doivent faire l'objet d'une attention particulière. Cela implique de renforcer la surveillance humaine et technologique, de contrôler les accès aux zones sensibles, de détecter rapidement les comportements suspects et de sécuriser les points stratégiques. La coordination entre opérateurs, forces de sécurité et autorités publiques est également essentielle pour garantir une réponse rapide et efficace en cas de menace ou d'incident.

- ***Infrastructures et réseaux ferroviaires***

Les transports ferroviaires constituent toujours une cible d'intérêt, à la symbolique et l'impact forts, même en cas d'attaque 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.

- ***Infrastructures et réseaux routiers et autoroutiers***

Les infrastructures et réseaux routiers et autoroutiers visent à garantir la continuité des déplacements, notamment dans le contexte de forte fréquentation estivale. Il s'agit d'augmenter la vigilance sur les axes structurants, en premier lieu en assurant la sécurité des zones particulièrement sensibles telles que les tunnels, et en prévenant les intrusions ou actes malveillants sur les sites techniques sensibles. Une attention particulière est portée à la coordination opérationnelle avec les forces de sécurité intérieure présentes sur le réseau routier, pour leur permettre une réaction rapide et efficace en cas de comportements atypiques, y compris sur les péages, les échangeurs et les aires.

- ***Spécificité du transport maritime de passagers***

Les exploitants des installations portuaires et les compagnies maritimes prendront les mesures nécessaires pour assurer la continuité du contrôle des véhicules, de leurs passagers et de leur chargement conformément aux textes en vigueur. A ce titre, tout exploitant d'une installation portuaire et tout exploitant d'un navire roulier à passagers mettra en place le dispositif de contrôle prévu par le plan de sûreté de l'installation et du navire, afin de prévenir l'introduction d'articles prohibés (armes à feu, explosifs, etc.) dans les terminaux d'embarquement et à bord.

3.1 consignes particulières :

Les consignes particulières de l'activité clé « transport », sur la période « été-automne 2026 », sont les suivants :

- surveillance renforcée des sites sensibles ;
- renforcement de la surveillance des parkings et des zones d'accès aéroportuaires ;
- contrôles aléatoires visibles en gares et stations ;

Chaque incident doit être considéré avec la plus grande attention.

4. Activités transverses - consignes particulières

4.1 Sensibilisation à la menace des attaques par véhicules-béliers

Les attaques par véhicules-béliers demeurent un mode d'action privilégié des organisations terroristes et des individus passant à l'acte de manière isolée. 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/vigipirate ;
- le guide du ministère de l'intérieur, accessible via le lien suivant : https://www.interieur.gouv.fr/documentation/ressources/securisation-des-evenements-de-voie-publique.html

4.2. 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 en appelant le 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 et sont accessibles sur le site internet du comité interministériel de prévention de la délinquance et de la radicalisation (CIPDR).

Je vous rappelle l'existence d'une boite mail structurelle référence s'agissant des problématiques de sûreté et qui a vocation à servir d'interlocuteur local : pref-vigipirate62@pas-de-calais.gouv.fr .

4.3. 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 biologiques et chimiques d'usage courant.

4.3.1 Cas particulier 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.

4.3.2 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 :

- Mail à pixaf@gendarmerie.interieur.gouv.fr

- Appel au ***01 78 47 34 96 (24/7).***

Deux fiches de bonnes pratiques du service central des armes et des explosifs (SCAE) relatives aux précurseurs d'explosifs et aux artifices et de divertissement peuvent utilement être consultées ou téléchargées sur le site du SGDSN, rubrique Vigipirate/fiches de recommandations et de bonnes pratiques/.

4.4. Lutte anti-drones

L'utilisation de drones s'impose désormais comme un moyen de nuisance répété en Europe. Elle constitue aussi une nouvelle arme de guerre, massive par la quantité, entre l'Ukraine et la Russie.

Les modes d'action les plus fréquents sont la captation d'informations sensibles à des fins de renseignement, la livraison par la troisième dimension d'objets prohibés en milieux sécurisés.

Ces engins disponibles très facilement et au pilotage accessible à tous permettent également de perpétrer des actes malveillants ou à caractère terroriste.

Les responsables de grands rassemblements doivent prendre en compte cette menace en menant une analyse de risques avec l'appui des référents sûreté locaux de la police ou de la gendarmerie nationales. De nombreux moyens mobiles de lutte anti-drones (LAD) sont désormais disponibles (héritage JOP 2024) et doivent systématiquement être déployés lors de rassemblements de personnes autorisés par les préfectures. Selon la sensibilité d'un événement et du niveau de menace, les forces de sécurité intérieure peuvent déployer des moyens de détection additionnels et des moyens de neutralisation des drones (brouillage, filets, destruction, etc.).

5 Information du grand public

La présente posture est la première mettant en œuvre le plan Vigipirate rénové. Cette évolution doit être considérée comme une opportunité de communiquer autour du plan Vigipirate et de relancer la dynamique de vigilance collective.

5.1. Efforts de communication

Vous êtes invité à mettre en place les logogrammes : « vigilance renforcée » sur vos structures.
Ces logogrammes peuvent être téléchargés sur le site du SGDSN à partir du lien suivant: https://www.sgdsn.gouv.fr/vigipirate/le-plan-vigipirate-faire-face-ensemble

5.2.Promotion des bonnes pratiques

Dans un souci de large diffusion des bonnes pratiques face à la menace terroriste, la version publique du plan Vigipirate « Faire Face Ensemble » peut être téléchargée sur le site du SGDSN (https://www.sgdsn.gouv.fr/vigipirate/le-plan-vigipirate-faire-face-ensemble).
Des fiches de sensibilisation sont également accessibles en ligne depuis l'espace Vigipirate du site Internet du SGDSN (https://www.sgdsn.gouv.fr/vigipirate/les-affiches-de-sensibilisation).
La communication des mesures et des comportements à adopter en cas d'attaque terroriste au sein des établissements et lieux recevant du public est fondamentale. Aussi, ces affiches peuvent être téléchargées et imprimées sur un format adapté au lieu où elles sont placées afin de les rendre visibles du public (privilégier les entrées et sorties des établissements, les halls 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). 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) :

Enfin, deux modules de formation en ligne 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.

6. La sécurité du numérique

Les mesures suivantes sont actives :

- Mesure NUM-SIC-002-2 : Créer des alertes de sécurité en analysant les journaux ou en activant des paramètres de supervision
- Mesure NUM-SIC-002-3 : Consulter régulièrement les sources d'information relatives aux mises à jour de sécurité, vulnérabilités et attaques (ex : site Internet du CERT-FR)
- Mesure NUM-SIC-002-11 : Valider et appliquer les mesures correctives
- Mesure NUM-SIC-002-12 : Evaluer et limiter la surface d'exposition (mesure proposée à l'activation)
- Mesure NUM-SIC-005-2 : Déterminer l'ensemble des composants du SI contenant un logiciel/matériel particulier
- Mesure NUM-SIC-001-1 : Absorber le trafic illégitime au niveau du réseau
- Mesure NUM-SIC-002-6 : Sensibiliser les utilisateurs sur un risque de sécurité et un comportement à adopter
- Mesure NUM-SIC-002-13 : Vérifier les annuaires de crise et le fonctionnement des moyens de communication sécurisés (mesure proposée à l'activation)
- Mesure NUM-SIC-002-14 : Adapter les dispositifs de réponse à incidents aux caractéristiques de la menace
-

- Mesure NUM-SIC-002-15 : Réaliser des tests de restauration des sauvegardes
- Mesure NUM-SIC-002-16 : Procéder régulièrement à un séquestre hors ligne exceptionnel des sauvegardes des systèmes les plus critiques (mesure proposée à l'activation)
- Mesure NUM-SIC-005-3 : Rechercher sur le SI des marqueurs particuliers correspondant à une attaque

Le détail des mesures cyber pour la sécurisation du numérique pourra vous être communiqué sur demande sur la boite fonctionnelle pref-vigipirate62@pas-de-calais.gouv.fr .

Mes services se tiennent à votre entière disposition pour vous apporter les précisions relatives à la mise en œuvre des mesures actives du plan Vigipirate.

Le préfet,

François-Xavier LAUCH