



**PRÉFET
DES CÔTES-
D'ARMOR**

*Liberté
Égalité
Fraternité*

**Cabinet
Service Interministériel
de Défense et de Protection Civile**

Saint-Brieuc, le 26 juin 2026

Service interministériel de défense et de protection civile



Le préfet des Côtes-d'Armor

à

Mesdames et Messieurs les maires
Madame et Messieurs les présidents
des établissements publics de
coopération intercommunale

Objet : Posture Vigipirate «été automne 2026 »

La nouvelle posture Vigipirate pour la période « été - automne 2026 » est active à compter du 22 juin 2026 et maintiendra l'ensemble du territoire national au niveau « urgence attentat ».

Cette posture rappelle les consignes en termes de vigilance à destination des représentants de l'autorité publique (militaires, policiers, gendarmes, surveillants pénitenciers, douaniers, etc.), et de protection des systèmes d'information face au risque d'attaques cybernétiques. En outre, il convient d'accorder une attention particulière à :

- la sécurisation des lieux placés sous votre autorité, le maintien du logogramme « urgence attentat » et la protection de leurs abords, notamment les établissements scolaires, d'enseignement supérieur et de recherche, les lieux de cultes les établissements de santé de première ligne et les lieux sujets à de fortes affluences ;
- la sécurisation des grands espaces de rassemblements, notamment les manifestations religieuses, sportives, sociales, culturelles ou politiques) se déroulant dans vos communes en invitant les organisateurs à adapter les mesures de sécurité qui leur incombent en adéquation avec la fréquentation saisonnière en portant une attention particulière aux abords des sites, ainsi qu'aux entrées et sorties des spectacles et rassemblements. Une extrême vigilance est requise, notamment pendant les périodes qui offrent une opportunité en termes de résonance médiatique ;
- le maintien d'un haut niveau de vigilance pour les établissements recevant du public, une vigilance particulière sera également accordée à la sécurité des palais de

justice et des établissements pénitentiaires dans le contexte de procès dits « signalés » et des transferts de détenus reconnus les plus dangereux. Cette vigilance sera renforcée lors des procès des personnes mises en cause pour faits de terrorisme. La sécurisation des juridictions abritant ces occurrences constituera un axe d'effort spécifique. Le contexte de sensibilité pour la vigilance sur les bâtiments judiciaires, outre le terrorisme, devra être élargi aux faits liés à la criminalité organisée ;

- les contrôles de l'accès des personnes à l'entrée des établissements d'enseignement (dont l'enseignement supérieur et la recherche) et des établissements de santé, médico-sociaux et sociaux est maintenu. Les dispositifs de sécurité des grands espaces de commerce privilégient la surveillance dynamique des espaces, la détection des comportements anormaux et le recours à la vidéosurveillance. Le contrôle systématique aux accès des espaces touristiques, culturels et de loisirs est à rechercher .
- le maintien de la vigilance dans le domaine des transports en milieu clos dotés de commerces (gares, ports etc.). Concernant le transport maritime, la présente posture prévoit la continuité du contrôle des véhicules, de leurs passagers et de leur chargement relatif aux conditions d'accès et de circulation en zone d'accès restreint des ports et des installations portuaires et à la délivrance des titres de circulation ;
- la menace associée aux attaques par véhicules-béliers est toujours d'actualité. Je vous demande par conséquent de veiller au renforcement des dispositifs de protection passive (plots, barrières, blocs en béton, etc.) mis en place sur les lieux et artères les plus fréquentés ainsi que lors de manifestations organisées par des opérateurs privés ;
- les menaces cybernétiques visant les administrations et les entreprises privées (attaques par rançongiciel, attaques indirectes et vulnérabilités critiques). Compte-tenu de la menace, il est nécessaire d'être extrêmement vigilant sur les potentielles vulnérabilités de vos réseaux informatiques, d'appliquer les correctifs de sécurité et d'avoir des sauvegardes non accessibles. Il convient de sensibiliser vos 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 des supports amovibles, de navigation internet ou d'échanges de courriels ;
- face aux menaces cyber, il convient de s'assurer du maintien de la capacité de communication entre les personnels en charge de la gestion de crise. Il est donc essentiel de s'assurer que les annuaires de crise, contenant les contacts du personnel pertinent en cas de crise, en interne comme en externe (bénéficiaires, partenaires), sont bien à jour et correctement diffusés à tous les acteurs. Par ailleurs, certaines menaces (notamment de type rançongiciel et DDoS) peuvent entraîner la perte des outils de communication usuels. Il est donc nécessaire de tester régulièrement les moyens de communication alternatifs et sécurisés, qui pourront être utilisés dans le cas d'une attaque impactant les outils de communication nominaux ;
- par ailleurs, l'utilisation des drones comme mode d'action régulièrement mis en œuvre pour capter des images ou diffuser des messages peut évoluer vers des actes de malveillance ou terroristes, notamment à l'occasion de grands rassemblements.

Les organisateurs doivent prendre en compte cette menace en sollicitant l'avis des référents sûreté locaux des forces de l'ordre ;

Tout comportement suspect doit être rapporté aux forces de l'ordre en composant le 17.

Je vous rappelle que plusieurs guides de bonnes pratiques et des référentiels adaptés aux secteurs d'activité concernés sont disponibles sur les sites suivants :

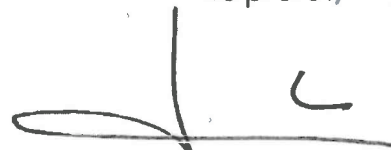
- <http://www.sgdsn.gouv.fr/vigipirate>
- <http://www.interieur.gouv.fr>
- <http://www.culturecommunication.gouv.fr>
- <http://www.ssi.gouv.fr>
- <https://secnumacademie.gouv.fr>

Dans un souci de large diffusion des bonnes pratiques face à la menace terroriste, des fiches de sensibilisation à destination, tant du grand public que des professionnels sont accessibles en ligne sur l'espace dédié du Gouvernement :

<https://www.sgdsn.gouv.fr/vigipirate/les-fiches-de-recommandations-et-de-bonnes-pratiques> et
<https://www.sgdsn.gouv.fr/vigipirate/les-guides>

Je vous remercie de votre implication.

Le préfet,



François de KEREVER

