

Paris, le 16 juillet 2016



COMMUNICATION relative à l'adaptation de la posture VIGIPIRATE

Objet : Adaptation anticipée de la posture VIGIPIRATE à la période estivale.

La nouvelle posture VIGIPIRATE qui intervient après l'attentat perpétré à Nice le 14 juillet 2016, vient adapter sans délais le dispositif de protection mis en œuvre dans le cadre de l'EURO 2016 au contexte particulier de la période estivale.

Cette posture d'application immédiate sera réévaluée durant la deuxième quinzaine du mois d'août, de manière à porter les ajustements nécessaires à la sécurisation de la rentrée scolaire.

Le niveau « alerte-attentat » a été déclenché dans la nuit du 14 au 15 juillet 2016 pour le département des Alpes-Maritimes et est maintenu en Île-de-France. La « vigilance renforcée » continue de s'appliquer sur le reste du territoire national.

Cette révision de posture répond à une menace qui demeure à un niveau particulièrement élevé, comme le démontre l'attentat perpétré à Nice, qui souligne encore la variété des modes d'action mis en œuvre par les terroristes. Cette posture traduit une bascule d'effort vers les lieux de villégiature touristiques. Elle met l'accent sur :

- la protection des sites touristiques et des grands événements estivaux susceptibles de générer une forte affluence, notamment les festivals ;
- le maintien de la vigilance dans le domaine des transports notamment au moment du « chassé-croisé » du début du mois d'août et lors de la fin de la période estivale ;
- le maintien dans la durée du dispositif de contrôle aux frontières ;
- la poursuite d'une démarche de sensibilisation permettant de renforcer la vigilance du grand public.

Concernant la culture, la plus grande vigilance doit être portée sur les concentrations de population (notamment les manifestations festives et les établissements recevant du public). Les grands rassemblements de personnes doivent être signalés aux préfetures concernées et les organisateurs doivent veiller à assurer une sécurité optimale en lien avec les forces de l'ordre.

La plus grande vigilance doit également porter sur les principaux sites culturels, historiques et touristiques rencontrant une forte affluence durant l'été.

En matière de protection des zones accueillant du public en extérieur, une attention particulière sera portée au contrôle des accès ainsi qu'au dispositifs passifs permettant, le cas échéant, d'y restreindre ou d'y interdire la circulation.

L'ensemble des actions de vigilance, de surveillance et de contrôle est récapitulé dans le tableau ci-dessous (réf : plan VIGIPIRATE mesures publiques).

Mesure	Commentaires
Activer les cellules de veille et d'alerte et les cellules de crise	Les cellules de crise des ministères sont activées en tant que de besoin.
Diffuser l'alerte au grand public	<ul style="list-style-type: none"> - affichage du logo « VIGIPIRATE Alerte-attentat » en Île-de-France et dans le département des Alpes-Maritimes et « VIGILANCE » hors Île-de-France, aux endroits où des mesures de protection renforcées sont mises en œuvre ; - diffusion de messages d'appel à la vigilance dans les établissements recevant du public (ERP), y compris en langues étrangères ; - information claire des visiteurs et spectateurs sur les sites web de chaque établissement concernant les mesures de contrôle en vigueur ; - information claire et visible à l'entrée de l'établissement : utiliser les pictogrammes en ligne sur le site http://www.culturecommunication.gouv.fr/Actions-de-renforcement-et-de-surveillance-des-lieux-culturels - application smartphone SAIP d'alerte aux populations - principalement conçue pour diffuser les alertes sur des attentats - entrée en service en juin 2016
Renforcer la surveillance et le contrôle	<p>Manifestations en extérieur</p> <p><i>1) dans une enceinte close d'un établissement :</i></p> <ul style="list-style-type: none"> - contrôle visuel <u>systématique</u> des visiteurs en demandant à ceux ayant des vêtements amples, susceptibles de dissimuler une arme automatique, de les ouvrir ;

	<p>- interdiction des valises et des sacs de grande contenance.</p> <p><u>Toute personne refusant le contrôle doit se voir interdire l'entrée de l'établissement.</u></p> <p>2) sur la voie publique : ces manifestations sont soumises à des restrictions qui peuvent être plus importantes selon les directives préfectorales.</p> <p>Ces dispositions ne font pas obstacle à la liberté de l'organisateur de renoncer à la tenue d'une manifestation dès lors qu'il le juge nécessaire, soit parce qu'il estime ne pas être en mesure de satisfaire pleinement à ses obligations de sécurité du public, soit en fonction de circonstances spécifiques liées notamment à la thématique de la manifestation. Un contact avec les services de police locaux peut aider les organisateurs dans leur appréciation du risque.</p> <p>Un effort particulier de vigilance doit porter sur les rassemblements liés aux grands événements estivaux, tels les festivals, et sur les sites touristiques estivaux, notamment culturels.</p>
Restreindre voire interdire le stationnement et/ou la circulation aux abords des installations et bâtiments désignés	<p>A l'appréciation des préfets pour le ciblage.</p> <p>En accord avec les forces de police, des mesures de sécurité passive peuvent utilement être déployées : barriérage, plots béton, chicane...</p>
Renforcer la surveillance aux abords des installations et bâtiments désignés	<p>Prioritairement pour les ERP, renforcement de la vigilance externe par l'installation de dispositifs de vidéoprotection.</p>
Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier)	<p>1) renforcement du contrôle des visiteurs / spectateurs :</p> <ul style="list-style-type: none"> - pour les établissements équipés de portiques : passage <u>systématique</u> sous portique ; - pour les établissements équipés de magnétomètres : utilisation <u>systématique</u>. <p>- valises et sacs de grande contenance : interdits dans les ERP non équipés de scanner à rayons X.</p> <p>Pour les établissements concernés, il convient d'informer le public (site web et affichage) de cette mesure, et de modifier le règlement intérieur de l'établissement.</p> <p><u>Toute personne refusant l'un de ces contrôles doit se voir interdire l'entrée de l'établissement.</u></p> <p>Toutefois, pour les chefs d'établissement de l'enseignement supérieur du secteur de la culture qui reçoivent des étudiants, ces derniers peuvent, selon la situation de leur établissement, autoriser leurs professeurs et leurs étudiants à introduire des valises, des sacs et des étuis d'instruments de musique après contrôle visuel du contenu.</p> <p>2) pour le personnel : badge (ou pièce d'identité) obligatoire pour l'accès à l'établissement. A l'appréciation des chefs d'établissement et selon la situation de leur établissement, autorisation est donnée à ceux-ci de procéder au renforcement des contrôles (inspection visuelle des sacs)</p>

	<p>pour les personnels des manifestations extérieures, les prestataires extérieurs, les personnels intérimaires et temporaires, et en tant que de besoin selon la taille, la configuration, le site ou le caractère symbolique de l'établissement, pour les personnels permanents, après information/consultation du CHSCT spécial d'établissement consacré aux mesures de sûreté et de sécurité.</p> <p>3) limitation des accès aux sites :</p> <ul style="list-style-type: none"> - accès visiteurs : limitation du nombre d'accès à l'initiative des chefs d'établissement ; - autres accès : les accès réservés à du personnel spécifique (artistes, prestataires extérieurs, agents de l'établissement) doivent faire l'objet d'un renforcement des contrôles tel qu'indiqué ci-dessus. <p>4) véhicules entrants : contrôle <u>systematique</u> et vérification de la marchandise.</p> <p><i>Ces contrôles doivent être le plus visible possible.</i></p>
Protéger logiquement ses systèmes d'information	<p>1) <u>Conseils aux utilisateurs</u></p> <ul style="list-style-type: none"> - demeurer vigilant sur les courriels reçus et, en cas de doute, ne pas ouvrir les pièces jointes ni cliquer les liens internet y figurant ; - limiter les navigations vers des sites internet n'ayant pas de rapport avec l'activité professionnelle ; - rendre compte aux responsables locaux de la sécurité des systèmes d'information de tout comportement anormal du poste de travail ; <p>2) <u>Conseils aux responsables organiques</u></p> <ul style="list-style-type: none"> - assurer une revue des droits des comptes les plus privilégiés et en assurer une supervision ; - contrôler l'application de la politique des mots de passe et renouveler les mots de passe des comptes les plus privilégiés ; - vérifier ou mettre en place les mesures de prévention en matière de déni de service. <p><i>Vous pouvez consulter les notes d'information et les guides de l'ANSSI sur le site www.ssi.gouv.fr/administration/bonnes-pratiques/ concernant notamment :</i></p> <ul style="list-style-type: none"> - <i>les dénis de service (prévention et réaction)</i> - <i>les défiguration de type web</i> - <i>les bons réflexes en cas d'intrusion sur un système d'information</i> - <i>la protection des sites internet</i>

Trois guides de bonnes pratiques sont à votre disposition sur le site du ministère :

<http://www.culturecommunication.gouv.fr/Actions-de-renforcement-et-de-surveillance-des-lieux-culturels>

- **guide à destination des organisateurs de rassemblements et festivals culturels**
- **guide à destination des dirigeants de salles de spectacle, de cinémas ou de cirques**
- **guide à destination des dirigeants d'établissements culturels patrimoniaux (musées, monuments historiques, archives et bibliothèques)**

Enfin, il convient de rappeler à vos collaborateurs appelés à effectuer des missions à l'étranger de consulter préalablement le site du ministère des affaires étrangères <http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/>