PRÉFET
DES ALPES-
MARITIMES
Liberté
Égalité
Fraternité

Cabinet

Direction des sécurités

Service interministériel de défense et de protection civiles

Nice, le - 5 MARS 2021

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

(pour instruction et information aux destinataires in fine)

Objet : Adaptation de la posture VIGIPIRATE - Changement de niveau d'alerte.

Réf. : - Plan gouvernemental VIGIPIRATE du 1er décembre 2016 (édition mai 2019).
- Circulaire du préfet des Alpes-Maritimes du 30 octobre 2020 relative à l'adaptation de la posture VIGIPIRATE « **attentat de Nice** » - Rehaussement au niveau 3 « Urgence Attentat ».

P. J. : - Fiche pratique : Hameçonnage ;
- Nouvelle plaquette VIGIPIRATE « faire face ensemble »;
- Logo VIGIPIRATE « sécurité renforcée-risque attentat ».

Considérant que l'état de la menace terroriste sur le territoire national, tout en restant à un niveau élevé, est devenu moindre qu'à la fin de l'année 2020, le Premier ministre a décidé de ramener le niveau 3 d'alerte VIGIPIRATE, actuellement en vigueur, au **niveau 2** du plan VIGIRATE : « **sécurité renforcée – risque attentat** », à compter du **5 mars 2021**.

Cette adaptation s'appuie sur la posture du plan VIGIPIRATE « **Automne Hiver 2020 – Printemps 2021**» du 26 octobre 2020.

Il n'a pas été fixé de date de fin à cette posture afin d'en assurer un renouvellement ou une adaptation

147, boulevard du Mercantour – 06286 NICE CEDEX 3
http://www.alpes-maritimes.pref.gouv.fr

au moment jugé le plus opportun.

Elle est, par ailleurs, susceptible d'être adaptée, en urgence, en cas d'événement grave ou d'évolution significative de la menace terroriste.

Dans le contexte de la crise sanitaire, les mesures de cette posture adaptent le dispositif en mettant l'accent sur :

- la sécurité des espaces de commerce, les activités relancées et les lieux rouverts au public à terme ;
- la sécurité des lieux de culte, des sites touristiques et des transports publics de personnes, en particulier lors des vacances scolaires et universitaires ;
- la sécurité des bâtiments publics (services publics, locaux associatifs ou politiques, écoles et universités), avec une attention particulière sur les établissements de santé, médico-sociaux et sociaux, ainsi que sur la sécurité des sites de production, de stockage et de distibution de produits de santé, y compris les centres de vaccination.

I- La sécurité des espaces de commerce, les activités relancées et les lieux rouverts au public à terme

Considérés comme des cibles privilégiées, la sécurité de ces lieux devra être maintenue. Les exploitants et les gestionnaires de ces espaces et de ces lieux sont invités à adapter les mesures de sûreté qui leur incombent et à sensibiliser leurs salariés aux bons comportements à adopter en cas de situation suspecte ou de menace terroriste.

Je rappelle qu'il leur revient de renforcer les échanges d'information avec les forces de sécurité intérieure et d'adapter les dispositifs de sécurité en privilégiant la surveillance dynamique des espaces, la détection des comportements anormaux et le recours à la vidéosurveillance.

Pour être pleinement efficaces, les points de filtrage aux entrées de site doivent disposer de moyens de communication et de procédures d'alerte de façon à réduire les délais d'intervention des forces de sécurité intérieure en cas d'événement.

II- La sécurité des lieux de culte, des sites touristiques et des transports publics de personnes, en particulier lors des vacances scolaires et universitaires

- Les lieux de culte :

La sécurité devra être renforcée autour des lieux de culte avec un effort sur la présence visible des forces de l'ordre, notamment lors des fêtes catholiques de Pâques, des fêtes juives de Pessa'h et du Ramadan par la mise en oeuvre de mesures de contrôle aux accès des lieux de rassemblement, en liaison avec les autorités religieuses locales.

- Sites touristiques :

Dans le cas où la situation sanitaire et épidémiologique de notre département le permettrait les lieux rouverts qui seraient sujets à de forte affluences saisonnières durant les vacances scolaires *(salles de spectacles, stations de sport d'hiver, ...)* bénéficieront de moyens adaptés en concertation avec les services de l'Etat (forces de sécurité intérieure – unités Sentinelle).

- Les transports publics de personnes :

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, ...*).

Je vous rappelle que la menace visant les emprises des gares, des aérogares et des stations de tramway impose une vigilance quotidienne et redoublée sur les espaces d'accueil des voyageurs, notamment durant les périodes d'affluence.

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

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 grande vitesse, réseaux-interurbains, ...)* doit faire l'objet d'une communication immédiate aux forces de sécurité intérieure 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
- mèl : permanence.cmvoa@developpement-durable.gouv.fr

Concernant le transport maritime de passagers, il est recommandé aux exploitants portuaires d'assurer la continuité du contrôle des véhicules, de leurs passagers et de leur chargement.

III- La sécurité des bâtiments publics, des établissements de santé, médico-sociaux et sociaux, ainsi que sur la sécurité des sites de production, de stockage et de distibution de produits de santé

Il s'agit des bâtiments hébergeant des services publics, des locaux associatifs ou politiques, écoles et universités mais aussi les établissements de santé *(hopitaux, cliniques...)*, médico-sociaux et sociaux *(EHPAD, foyers...)*. De même l'ensemble des sites participant à la production, au stockage et à la distribution de produits de santé ainsi que les centres de vaccination.

Je vous demande d'actualiser les annuaires de crise et les procédures d'alerte afférentes de même que les plans de protection et les procédures internes d'évacuation ou de confinement devront être portés à la connaissance des nouveaux arrivants.

Durant la période des élections départementales et régionales prévues en juin prochain une vigilance particulière devra être portée aux bureau de vote.

Malgré les préconisations actuelles liées à la crise sanitaire *(port du masque, distanciation physique, limitation du brassage de la population, ...)* ces consignes ne doivent pas conduire à abaisser le niveau de sécurisation et de contrôle des flux de personnes, notamment lorsqu'il s'agit de rassemblements organisés au sein et/ou aux abords des établissements, d'événements sportifs, de déplacements sur le temps scolaire et hors du temps scolaire, y compris les activités organisées par les structures d'accueil collectif de mineurs.

Il est impératif de maintenir une surveillance active et un contrôle pertinent des accès aux différentes emprises bâtimentaires.

Les attroupements seront réduits au minimum et les stationnements sauvages aux abords des établissements seront empêchés avec le concours des forces de sécurité.

Afin de contribuer pleinement à l'action coordonnée de l'ensemble des administrations dans le département, au regard des problématiques de sûreté, de sécurité, et plus encore, d'anticipation et de gestion de crise, le partage d'information entre les différents acteurs doit se traduire concrètement par :

- la participation des différents acteurs aux projets de sécurisation des services et des établissements;
- le déploiement de procédures partagées des chaînes d'alerte et de gestion de crise;
- la mise à jour et communication des plans particuliers de mise en sûreté (PPMS) «attentat-intrusion» et des plans bâtimentaires ;
- la mise en oeuvre d'exercices communs.

Les établissements de santé, sociaux et médico-sociaux demeurent des cibles particulièrement vulnérables. La vigilance doit donc restée élevée notamment pour les établissements de santé, médico-sociaux et sociaux, ainsi que pour les sites de production, de stockage et de distribution de produits de santé, y compris les centres de vaccination.

IV- Consignes de sécurité et de vigilance

- Sensibilisation des personnes en tenue :

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

- Sensibilisation aux risques cyber :

A la suite du déclenchement de la pandémie de COVID-19, le recours intensif au télétravail et aux outils numériques a rendu plus vulnérables les utilisateurs connectés à distance au système d'information de leur organisation. Ceci a eu pour effet une augmentation de la surface d'attaque par la mise en service de nouveaux moyens de connexion à distance en urgence conduisant parfois à une insuffisance de la prise en compte de la sécurité.

A cet effet, je vous invite à consulter la fiche conseil jointe en annexe.

Vous veillerez aussi à la sensibilisation du public accueilli dans vos locaux par l'affichage du logo correspondant au niveau du plan VIGIPIRATE actuellement en vigueur sur le territoire national, un exemplaire est joint à la présente circulaire. Il doit être apposé, de faço visible, à l'entrée, dans les halls d'accueil et les lieux de passage du public.

Enfin, je vous rappelle que le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN) a développé une **plateforme de sensibilisation VIGIPIRATE**. Il s'agit d'un outil pédagogique accessible au plus grand nombre qui contribue à favoriser une éducation citoyenne en matière de sécurité nationale.

Ce site a été mis en ligne à l'adresse suivante : www.vigipirate.gouv.fr.

Je vous recommande vivement de le consulter et vous encourage à diffuser l'information à l'ensemble des agents et des personnels placés sous votre autorité.

Le préfet des Alpes-Maritimes

Bernard GONZALEZ

Liste des destinataires *in fine* de la circulaire

- Monsieur le préfet délégué ;
- Monsieur le secrétaire général de la préfecture des Alpes-Maritimes ;
- Madame la sous-préfète de l'arrondissement de Grasse ;
- Monsieur le directeur de cabinet du préfet ;
- Monsieur le sous-préfet de Nice montagne ;
- Madame la sous-préfète chargée de mission ;
- Monsieur le recteur de l'académie de Nice ;
- Monsieur le procureur de la République de Nice ;
- Madame la procureure de la République de Grasse ;
- Madame le contrôleur général, directrice départementale de la sécurité publique ;
- Monsieur le colonel, commandant le groupement de gendarmerie des Alpes-Maritimes ;
- Monsieur le contrôleur général, directeur départemental des services d'incendie et de secours ;
- Monsieur le lieutenant-colonel, délégué militaire départemental ;
- Monsieur le directeur départemental de la sécurité intérieure ;
- Monsieur le chef du service départemental du renseignement territorial ;
- Monsieur le chef du service de police judiciaire de Nice ;
- Monsieur le commandant du RAID 06 ;
- Madame la directrice départementale de la police aux frontières ;
- Monsieur le président de l'aéroport Nice-Côte d'Azur ;
- Monsieur le commandant la compagnie de gendarmerie des transports aériens ;
- Monsieur le commandant la CRS N°06 ;
- Monsieur le directeur des services départementaux de l'éducation nationale ;
- Monsieur le président de l'université Nice Sophia-Antipolis ;
- Monsieur le président de l'association des maires du département des Alpes-Maritimes ;
- Monsieur le président de l'association des maires ruraux du département des Alpes-Maritimes ;
- Monsieur le directeur départemental des territoires et de la mer ;
- Monsieur le directeur départemental de la cohésion sociale ;
- Madame la directrice départementale de la protection des populations ;
- Monsieur le délégué départemental de l'agence régionale de santé ;
- Madame la cheffe de l'unité départementale de la direction régionale de l'environnement, de l'aménagement et du logement (DREAL) ;
- Monsieur le chef du centre de déminage de Nice ;
- Monsieur le directeur de la sécurité de l'aviation civile Sud-Est ;
- Monsieur le chef du service de la navigation aérienne Sud-Est ;
- Monsieur le responsable régional sûreté de la SNCF ;
- Mesdames et Messieurs les dirigeants et responsables des régies de transport public routier des Alpes-Maritimes ;
- Messieurs les exploitants portuaires ;
- M. l'évêque de Nice ;
- M. le président du consistoire régional de Nice ;
- M. le vice-président et délégué départemental du conseil régional du culte musulman ;
- M. le président du pôle départemental de la fédération protestante ;
- M. le représentant local de la conférence des évêques orthodoxes de France .

SÉCURITÉ DU NUMÉRIQUE
L'HAMEÇONNAGE (OU PHISHING)

VIGIPIRATE

Cible : personnels des organismes privés et publics

1 Et si c'était vous ?

Ingénierie sociale

Alors que vous assurez la permanence pendant les fêtes de fin d'année, un individu vous contacte par téléphone. Il souhaite obtenir rapidement, pour motif professionnel, les codes d'accès de l'application financière en charge des paiements fournisseurs et des salaires. À force d'arguments et grâce à un ton assuré, il réussit à vous convaincre et, en l'absence de votre hiérarchie, vous cédez sous la pression et lui communiquez l'information convoitée.

S'il ne s'agit pas d'une attaque informatique directe mais d'une technique répandue d'ingénierie sociale, ce type d'information (code d'accès, coordonnées bancaires, données personnelles, etc.) peut être utilisé comme point d'entrée pour mener une attaque à l'encontre de votre organisme.

Attaque par la messagerie

Au retour d'une absence prolongée du bureau, vous trouvez votre messagerie électronique engorgée. Pressé, vous ignorez l'invitation à redémarrer votre ordinateur et empêchez par conséquent l'installation des mises à jour. En parcourant rapidement les objets de vos courriels, l'un d'eux semble traiter d'affaires en cours vous concernant directement et retient votre attention. Vous l'ouvrez et y découvrez un bref message vous enjoignant de consulter un site Internet qui vous est familier dans l'exercice quotidien de vos fonctions.

Vous venez d'être victime d'hameçonnage (ou *phishing*).

En contrevenant à un principe d'hygiène fondamental (mettre à jour ses logiciels) et en cliquant sur ce lien d'apparence légitime sans prêter attention à certains détails, vous avez permis à un attaquant d'installer un programme malveillant dans le système d'information de votre entreprise et vous lui avez donné accès non seulement à vos dossiers mais aussi à ceux de vos collègues.

2 Comment renforcer ma vigilance et bien me protéger ?

Qu'est-ce que l'hameçonnage ?

L'hameçonnage est une technique d'attaque prenant la forme d'un courriel qui vous est adressé et qui semble provenir d'un expéditeur de confiance. Ce courriel peut contenir un **fichier**, une **pièce jointe** ou un **lien de redirection vers un site frauduleux**, avec une incitation à cliquer sur ces éléments, ce qui permettra à l'attaquant de recueillir de l'information ou d'installer un programme malveillant dans le système d'information de votre organisme.

VIGIPIRATE

SÉCURITÉ DU NUMÉRIQUE
L'HAMEÇONNAGE (OU PHISHING)

Adopter les bonnes pratiques au quotidien

- Méfiez-vous des courriels exigeant de vous une réponse ou une action immédiate et vous intimant de ne pas en informer votre hiérarchie ou vos collaborateurs.
- Soyez prudents vis-à-vis des courriels comportant des visuels a priori officiels mais dont la résolution est mauvaise.
- Ne cliquez jamais sur un lien ou une pièce jointe dont l'origine ou la nature vous semblent douteuses. **Au moindre doute, privilégiez l'accès au site web en tapant directement l'adresse** dans la barre de recherche.
- Soyez à l'affût des fautes d'orthographe ou de syntaxe dans l'adresse de l'expéditeur, l'objet du courriel ou le corps du texte.
- Ne répondez jamais à un courriel vous demandant des informations confidentielles (identifiants, coordonnées bancaires, etc.). **Au moindre doute, n'hésitez pas à contacter l'expéditeur** par un autre canal, par exemple téléphonique.
- Méfiez-vous des courriels d'expéditeur connu mais dont l'adresse électronique ou la nature du message sont inhabituelles ou catégorisés comme « spam / indésirable » par le logiciel de messagerie.
- Procédez régulièrement au redémarrage de votre poste, notamment lorsque le système vous y invite.

3 Je pense avoir été victime d'une attaque. Que faire ?

Qui prévenir ?

Si vous pensez avoir été victime d'une attaque informatique :

- prévenez immédiatement le support informatique de votre organisme et vos supérieurs hiérarchiques ;
- procédez sans délai au renouvellement de vos identifiants si vous les avez transmis lors de l'attaque.

4 Documents de référence

Guide des bonnes pratiques de l'informatique
http://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

Maquette et impression : Pôle Conception graphique-Fabrication – DSAF/DPL – Octobre 2017.

PREMIER MINISTRE
Liberté
Égalité
Fraternité

FAIRE FACE ENSEMBLE

À tout moment, rester vigilant !
rendez-vous sur : https://vigipirate.gouv.fr

SOYEZ VIGILANT AU QUOTIDIEN

Appropriez-vous votre environnement et sachez alerter lorsque vous êtes témoin d'une incohérence.

CYBERVIGILANCE : ADOPTEZ LES BONS REFLEXES

CYBER MALVEILLANCE GOUV.FR
Assistance et prévention en sécurité numérique

Conseils et assistance sur :
cybermalveillance.gouv.fr

PRÉVENIR, C'EST PROTÉGER

Lorsqu'une combinaison d'indices laisse présager d'une radicalisation.
stop-djihadisme.gouv.fr

0 800 005 696 Service & appel gratuits

FORMEZ-VOUS AU SECOURISME

Soyez capable d'alerter les secours, procéder à un massage cardiaque ou traiter les hémorragies.

https://gouvernement.fr/risques/se-former-aux-premiers-secours

PRÉPAREZ VOTRE VOYAGE

« conseils aux voyageurs » sur :
diplomatie.gouv.fr

inscription sur le site ARIANE :
pastel.diplomatie.gouv.fr/fildariane

17
POLICE SECOURS

112
NUMÉRO D'APPEL D'URGENCE EUROPÉEN

114
NUMÉRO D'URGENCE POUR LES PERSONNES SOURDES ET MALENTENDANTES

PREMIER MINISTRE
Liberté
Égalité
Fraternité

Réagir en cas d'attaque

1. S'ÉCHAPPER

ÊTES-VOUS CERTAIN DE POUVOIR VOUS ÉCHAPPER SANS RISQUE ?

SI OUI

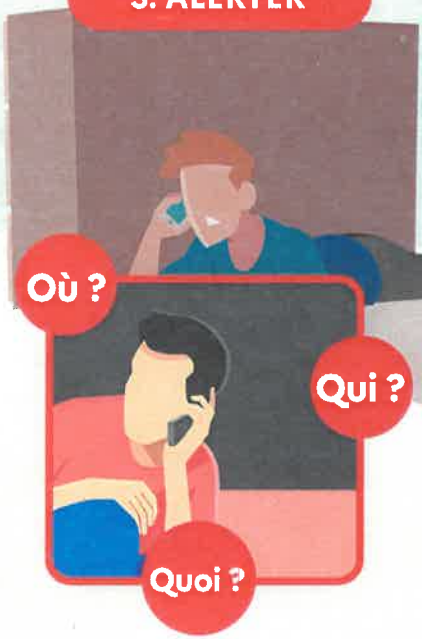
- Ne déclenchez pas l'alarme incendie
- Laissez toutes vos affaires sur place
- Ne vous exposez pas (courbez-vous)
- Prenez la sortie la moins exposée
- Utilisez un itinéraire connu
- Aidez les autres personnes à s'échapper
- Prévenez / alertez les personnes
- Évitez les mouvements de panique
- Facilitez l'intervention des forces de sécurité intérieure et des services de secours.

2. SE CACHER

SI NON ENFERMEZ-VOUS ET BARRICADEZ-VOUS

- Enfermez-vous et barricadez-vous
- éloignez-vous de la fenêtre
- Mettez les portables sur silencieux et décrochez les téléphones fixes
- Rassurez vos collègues
- Restez le plus silencieux et discret possible

3. ALERTER



UNE FOIS CACHÉ ET EN SÉCURITÉ, APPELEZ LES SECOURS

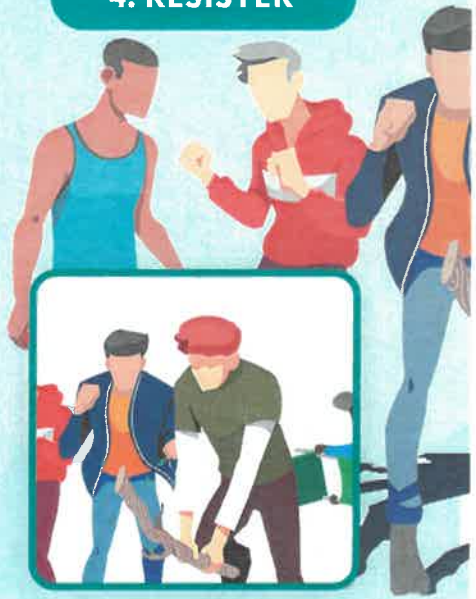
Où ? : Donnez votre position mais également celle de vos agresseurs.

Quoi ? : Nature de l'attaque (explosion, fusillade, attaque à l'arme blanche...)

Qui ? : Nombre d'assaillants, description physique et attitude, estimation du nombre de personnes blessées ou cachées.

- Comment se comportent-ils ?
- Regardent-ils la télé ?
- Quels moyens de communications ont-ils ?
- Ne raccrochez pas !

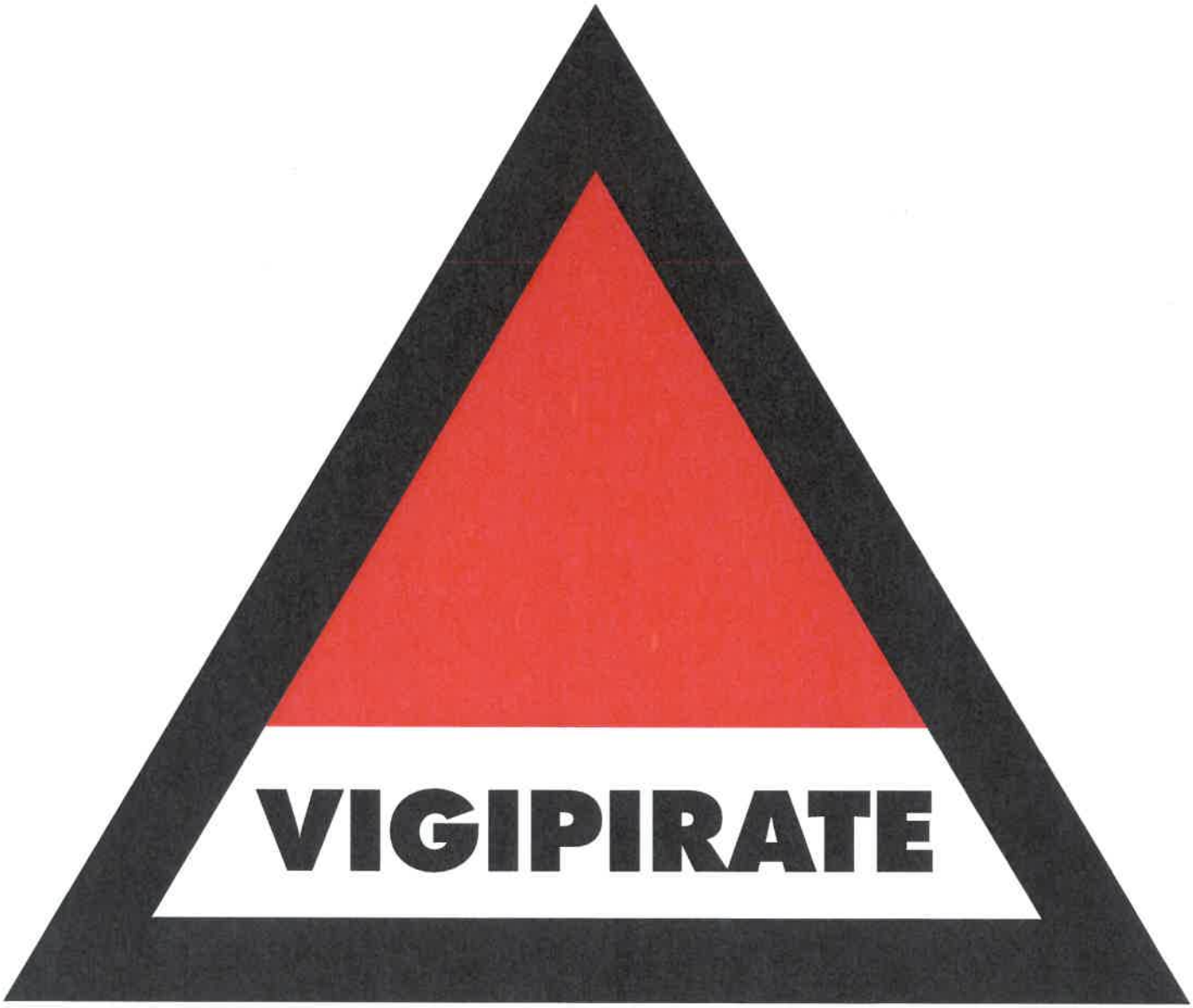
4. RÉSISTER



SI SE CACHER OU ÉVACUER EST IMPOSSIBLE, ET SI VOTRE VIE EST EN DANGER

- Tentez de neutraliser le terroriste à plusieurs.
- Distrayez l'adversaire (criez)
- Protégez-vous avec un bouclier de fortune (sac, vêtement enroulé autour de l'avant-bras).

FAIRE FACE ENSEMBLE



SECURITE RENFORCEE
RISQUE ATTENTAT