PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Direction de la protection et de la sécurité de l'Etat

Paris, le

N° /SGDSN/PSE

Le secrétaire général
de la défense et de la sécurité nationale
à
destinataires *in fine*

Objet : Adaptation de la posture VIGIPIRATE « Automne Hiver 2020 – Printemps 2021 ».

Références :
1. Plan gouvernemental Vigipirate n°10200/SGDSN/PSE/PSN/CD du 1er décembre 2016 (édition mai 2019).
2. Catalogue des fiches mesures Vigipirate (édition mai 2019).

Annexes :
1. Cartographie des attentats réalisés, échoués, déjoués en Europe de 2019 au 16 octobre 2020.
2. Historique des attentats en France de 2015 au 16 octobre 2020.
3. Fiche pratique : Hameçonnage.
4. Fiche pratique : chaine d'alerte face à une menace.
5. Fiche pratique : signalement de radicalisation.

Pièce jointe : Tableau actualisé des mesures Vigipirate.

La nouvelle posture Vigipirate « *Automne Hiver 2020 – Printemps 2021* » sera active à compter du 26 octobre 2020 et maintiendra l'ensemble du territoire national au niveau « ***sécurité renforcée - risque attentat*** ».

Dans le contexte de republication des caricatures de Mahomet par Charlie Hebdo le 2 septembre 2020, la menace terroriste demeure à un niveau élevé, comme l'illustrent les attaques du 3 janvier à Villejuif (94), du 4 avril à Romans-sur-Isère (26), du 27 avril à Colombes (92), du 25 septembre à Paris et du 16 octobre à Eragny (95). Cette posture Vigipirate adapte donc le dispositif en mettant l'accent sur :

- la sécurité des grands espaces de commerce, des lieux de rassemblement, tels que les marchés de Noël et les lieux de culte, marqués par une forte affluence lors des fêtes de fin d'année ;
- la sécurité des sites touristiques et des transports publics de personnes, en particulier lors des vacances scolaires et universitaires ;
- la sécurité des grands événements qu'ils soient sportifs, culturels ou commémoratifs ;
- la sécurité des bâtiments publics (services publics, locaux associatifs ou politiques), avec une attention particulière sur les établissements scolaires ainsi que sur les établissements de santé, médico-sociaux et sociaux, et la sécurité des sites de

production, de stockage et de distribution des produits de santé.

Après une description du contexte général et une évaluation de la menace, cette note de posture expose les différents objectifs de sécurité mais sans viser à être exhaustif. Chaque ministère en assurera sa déclinaison en prenant en compte sa vulnérabilité propre. Une version actualisée du tableau des mesures Vigipirate est jointe à la présente note.

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 l'ensemble des ministères.

SOMMAIRE

Avertissement : ce document pris dans son ensemble est classifié *confidentiel défense*. Les paragraphes commençant par [CD] sont classifiés, ceux commençant par [DR] sont protégés. L'ensemble des autres paragraphes, [NP] ou non marqués , est diffusable sans restriction.

1. [NP] Contexte général

1.1 Principaux événements sur le territoire national

La période couverte par la posture « *Automne Hiver 2020 – Printemps 2021* » est marquée par :

- les fêtes de fin d'année qui seront ponctuées par les célébrations religieuses et l'organisation sur l'ensemble du territoire national de marchés de Noël ;
- les élections régionales et départementales, au printemps 2021
- les flux importants de voyageurs dans les transports collectifs de personnes lors des vacances de la Toussaint, de Noël, d'hiver et de printemps ;
- la sécurité des grands événements qu'ils soient sportifs, culturels ou commémoratifs.
- les modalités de gestion de la crise du COVID 19.

Le contexte particulier de la crise COVID rend malheureusement impossible un récapitulatif des principaux événements (culturels, sportifs, religieux, commémoratifs, etc.). **Les mesures de sécurité sanitaires pour limiter la diffusion du virus, devront être évaluées par les autorités préfectorales** qui restent juges du niveau à atteindre pour encadrer la sûreté des manifestations à forte affluence ou au caractère symbolique marqué. La gestion des flux et des files d'attente devront ainsi faire l'objet d'une vigilance accrue.

1.2 Prolongation des contrôles aux frontières intérieures

La France a rétabli les contrôles aux frontières intérieures le 13 novembre 2015. Initialement prévu pour la durée de l'organisation de la COP 21 (Conférence des Nations-Unies pour le climat), c'est-à-dire du 13 novembre au 13 décembre 2015, le rétablissement de ces contrôles a, depuis, été régulièrement reconduit sur le fondement de l'article 25 du code frontières.

La France a informé la commission européenne de la reconduction du rétablissement des contrôles aux frontières intérieures jusqu'au 30 octobre 2020 du fait du niveau de menace mais aussi du contexte sanitaire. Si cette mesure ne devait pas être renouvelée, une information *ad hoc* serait transmise et les adaptations intégrées dans la posture.

1.3 Anticipation des conséquences liées au BREXIT

A la suite de la ratification de l'accord de retrait, le Royaume-Uni a quitté l'Union européenne le 31 janvier 2020 à minuit, devenant le 1er février 2020 un Etat tiers. Une période de transition de 11 mois s'est ouverte durant laquelle le Royaume-Uni a conservé un accès au marché intérieur et à l'union douanière.

Cette période, qui n'a pas été renouvelée, prendra fin le 31 décembre 2020 à minuit. L'application effective du retrait prendra effet le 1er janvier 2021.

Les conséquences en termes de voyageurs et de marchandises ont été anticipées par les administrations en charge des formalités et des contrôles frontaliers. Ainsi, la Direction générale des douanes et droits indirects, en lien avec ses partenaires, s'est préparée afin de garantir la continuité et la fluidité des flux de marchandises et de voyageurs entre la France et le Royaume-Uni. Un dispositif de "*frontière intelligente*"[1], reposant sur l'anticipation et la dématérialisation des formalités douanières, a notamment été élaboré.

[1] La frontière intelligente est une interface permettant de faire dialoguer les applicatifs de dédouanement avec les systèmes d'information des différents gestionnaires de sites partenaires. Pour un véhicule, une enveloppe logistique (qui contient les informations relatives aux formalités douanières) est générée par les opérateurs. Avec cette enveloppe et le numéro de plaque de d'immatriculation, un appairage est réalisé, ce qui permet d'aiguiller le véhicule dès son arrivée (zone verte : passage libre / zone orange : formalités à réaliser) afin de gérer le flux en temps réel. Plus d'informations sur le site https://www.douane.gouv.fr/dossier/franchissons-le-brexit-ensemble

1.4 Evolution du contexte juridique :

1.4.1 Nouvelles dispositions législatives et réglementaires

- Loi n° 2020-833 du 2 juillet 2020 relative au droit des victimes de présenter une demande d'indemnité au fonds de garantie des actes de terrorisme et d'autres infractions :
  - Modifie l'article 706-5 du code de procédure pénale.
- Décrets n° 2020-118 et n° 2020-119du 12 février 2020 renforçant les dispositions nationales de lutte contre le blanchiment de capitaux et le financement du terrorisme :
  - le décret n° 2020-118 est pris pour l'application des articles L. 561-2 à L. 561-50 du code monétaire et financier, dans leur rédaction issue de l'ordonnance n° 2020-115 du 12 février 2020 renforçant le dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme.
  - le décret n° 2020-119 est pris pour l'application des articles L. 561-2 à L. 561-50 du code monétaire et financier, dans leur rédaction issue de l'ordonnance no 2020-115 du 12 février 2020 renforçant le dispositif français de lutte contre le blanchiment et le financement du terrorisme. Ce décret précise les compétences de TRACFIN et élargit la composition du Conseil d'orientation de lutte contre le blanchiment de capitaux et le financement du terrorisme, renforce sa mission de coordination et précise les modalités de transmission des informations relatives au bénéficiaire effectif des personnes inscrites au RCS.

1.4.2 Autres dispositions

- Guide relatif à la mise en œuvre des dispositions des articles L. 114-IV du code de la sécurité intérieure et L. 4139-15-1 du code de la défense (procédure de signalement pour radicalisation des agents publics exerçant des missions de souveraineté ou relevant de la sécurité ou de la défense).

1.4.3 Contentieux

Par une décision n° 2020-805 du 7 août 2020, le Conseil constitutionnel a reconnu que l'objectif de lutte contre le terrorisme participe de l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public.

Il a toutefois considéré qu'était contraire à la Constitution l'article 1er de la loi instituant une mesure de sûreté prévue par l'article 706-25-15 du code de procédure pénale, visant à soumettre des auteurs d'infractions terroristes, dès leur sortie de détention, à des obligations et interdictions afin de prévenir leur récidive.

Il a en effet estimé que :

- la mesure de sûreté méconnaissait la liberté d'aller et venir, le droit au respect de la vie privée et le droit de mener une vie familiale normale (obligation d'établir sa résidence dans un lieu déterminé, obligation de se présenter périodiquement aux services de police ou aux unités de gendarmerie nationale jusqu'à trois fois par semaine etc.) ;
- la durée de la mesure en accroît la rigueur (cinq voire dix ans) ;
- la mesure peut être prononcée dès lors que la partie ferme de la peine est au moins égale à trois mois d'emprisonnement ;
- il n'est pas exigé que la personne ait pu, pendant l'exécution de sa peine, bénéficier de mesures de nature à favoriser sa réinsertion ;

Les renouvellements de la mesure de sûreté peuvent être décidés aux mêmes conditions que la décision initiale sans qu'il soit exigé que la dangerosité de la personne soit corroborée par des éléments nouveaux ou complémentaires.

2 [CD]

3 [NP] Evaluation des principaux risques cyber sur la période couverte

3.1 Impacts de la crise sanitaire et retour de congés

À 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 car isolés de leur environnement professionnel. Ainsi, des attaques par hameçonnage (courriels avec lien ou pièce jointe malveillante) ont été menées à des fins de captation de données ou de chantage par rançongiciel. Ce recours intensif au télétravail a entrainé une augmentation de la surface d'attaque par la mise en service de nouveaux moyens de connexion à distance aux systèmes d'information en urgence ce qui a conduit parfois à une insuffisance de la prise en compte de la sécurité.

Le retour au travail en présentiel ainsi que le retour de congés, constituent également des périodes particulièrement critiques et propices aux attaques informatiques. Les attaquants exploitent régulièrement la baisse de vigilance des utilisateurs associée au traitement et à l'échange important de courriels (offres promotionnelles, *etc.*).

De plus, lors de ces périodes, les missions de détection et de réponse aux incidents de sécurité ou de mise à jour des logiciels et des systèmes d'information peuvent être complexifiées par des effectifs restreints voire l'absence des équipes de sécurité informatique.

3.2 Tendances actuelles et vulnérabilités critiques

3.2.1 Attaques par rançongiciel

En 2020, les attaques par rançongiciel, menées par des groupes cybercriminels, ont fortement augmenté et de manière plus ciblée. Elles touchent autant des organisations publiques (ex : collectivités locales et établissements de santé) que des entreprises privées (énergie, BTP, technologies, aéronautique).

De plus, l'épidémie du COVID-19 a donné lieu à une recrudescence de ces attaques notamment par le biais de courriels sur ce thème proposant des liens ou des pièces jointes malveillantes.

Ce dernier constat est renforcé, par la prolifération de rançongiciels accessibles aux cybercriminels disposant de faibles compétences techniques, d'une part, et le faible niveau de sécurité des systèmes d'information des entités victimes, d'autre part. La situation est aggravée par l'absence de préparation de nombreuses entités à une crise cyber majeure : absence de plan de gestion de crise, absence de plan de continuité et de reprise d'activité et lacunes dans les systèmes de supervision et des sauvegardes.

Depuis début 2020, de nombreux opérateurs du rançongiciel exploitent une nouvelle tactique pour maximiser leurs gains : un premier groupe d'attaquants réalise l'intrusion initiale et revend l'accès au second qui opère le rançongiciel. Profitant de cet accès, ce dernier exfiltre des données parfois sensibles de la cible. Après la séquestration des données et dans le cas où la rançon n'est pas payée, l'attaquant publie les données exfiltrées sur un site Internet.

En septembre 2020, l'ANSSI a constaté un ciblage d'entreprises et administrations françaises par le code malveillant Emotet. Il convient d'y apporter une attention particulière car Emotet est désormais utilisé pour déposer d'autres codes malveillants susceptibles d'impacter fortement l'activité des victimes.[2]

[2] https://www.ssi.gouv.fr/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/

3.2.2 Attaques indirectes (supply chain attack)

La tendance, identifiée en 2017, d'utilisation d'attaques indirectes, s'est confirmée en 2019. Plusieurs opérations d'espionnage informatique ont ciblé des organisations dans plusieurs secteurs d'activité dont celui de la santé et de l'énergie ainsi que des secteurs détenteurs de propriété intellectuelle (fleurons industriels). Face à des réseaux informatiques de plus en plus sécurisés, les attaquants s'orientent vers la compromission des liens de mises à jour des logiciels de leur cible finale, ou de réseaux de prestataires de services travaillant pour ces dernières.

3.2.3 Vulnérabilités critiques

Plusieurs vulnérabilités critiques ont encore été dévoilées depuis le début de l'année 2020. En janvier, le CERT-FR a alerté sur des attaques ayant exploité une vulnérabilité affectant des logiciels Citrix et plus récemment des logiciels d'équipements Cisco. Ces derniers permettent un accès distant aux ressources d'une organisation, nécessairement utilisés par des employés en itinérance ou en télétravail. D'autres vulnérabilités critiques dans des solutions d'accès distant ont été exploitées dans des attaques. Par exemple, l'exploitation des vulnérabilités des logiciels Pulse Secure VPN et Palo Alto Networks ont permis la compromission de systèmes d'information notamment à des fins d'exfiltration de données.

Lors de sa mise à jour mensuelle de janvier, Microsoft a publié deux correctifs de sécurité pour de multiples vulnérabilités critiques sur Windows. Celles-ci affectent plusieurs versions du système d'exploitation, dont plusieurs versions destinées aux serveurs, augmentant ainsi la surface d'exposition aux attaques des systèmes concernés. Ces vulnérabilités ont fait l'objet d'une adaptation en urgence de la posture Vigipirate en janvier 2020.

Plus récemment, de nouvelles vulnérabilités critiques ont également été publiées.

4 [NP] Adaptation de la posture Vigipirate « Automne Hiver *2020 – Printemps 2021 »*

La posture Vigipirate « *Automne Hiver 2020 – Printemps 2021 »,* active à compter du 26 octobre 2020, **maintient le territoire national au niveau « *sécurité renforcée - risque attentat* ».**

4.1 Sécurité des lieux de rassemblement et des lieux de culte

- *Contexte général*

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 sollicitée.

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 sus-cités. 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.

- *Objectifs de sécurité recherchés sur la période*
  - *Mesures propres aux fêtes religieuses*

La sécurité sera renforcée autour des lieux de culte avec un effort sur la présence visible des forces de l'ordre, notamment lors des fêtes catholiques de Noël et de Pâques, des fêtes juives de Pessa'h et du ramadan. En liaison avec les autorités religieuses locales, la mise en œuvre de mesures de contrôle des accès est recommandée.

  - *Mesures propres aux périodes de vacances scolaires*

Les lieux sujets à de fortes affluences saisonnières durant les vacances scolaires (salles de spectacles, marchés de Noël, stations de sport d'hiver, etc.) bénéficieront de moyens adaptés. Les services de l'État (forces de sécurité intérieure – unités Sentinelle) adapteront leur dispositif en conséquence. Les opérateurs seront incités à solliciter l'appui des référents sûreté départementaux de la police ou de la gendarmerie nationale.

  - *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/Actualites/L-actu-du-Ministere/Securisation-des-evenements-de-voie-publique.

4.2 Sécurité des grands espaces de commerce, de tourisme et de loisir

- *Contexte général*

Les lieux de commerce, les espaces de loisirs et les sites touristiques majeurs restent des cibles privilégiées.

La sécurité sera renforcée autour des grands espaces de rassemblements ayant pour objet des activités commerciales (marchés de Noël, salons d'expositions, foires, etc.), les interconnexions de transports en milieu clos dotées de commerces (métros, gares, etc.) demeureront également un point de vigilance.

Cette période incluant les fêtes de fin d'année appelle une vigilance accrue notamment sur le secteur du tourisme et des parcs de loisirs, particulièrement fréquentés au moment des vacances

scolaires. Enfin, la sécurité des grands espaces de commerce lors des soldes d'hiver, marquées par une forte affluence, demeure un axe d'attention majeur.

De façon plus générale, il revient aux autorités préfectorales d'évaluer le niveau de sécurité à atteindre pour les différentes activités sises dans leur département. Lorsque des éléments objectifs attestent d'une menace sur le plan local, ou qu'un événement révèle une vulnérabilité particulière, ceux-ci sont communiqués aux responsables de sûreté des établissements concernés afin de leur permettre d'adapter leur dispositif .

Cette démarche s'inscrit dans la volonté de renforcer les liens et la coordination entre acteurs publics et privés.

- *Objectifs de sécurité recherchés sur la période*

La sécurisation des grands espaces de commerce, des sites de tourisme et de loisirs passe, entre autres, par :

- *La sensibilisation des personnels :*

Elle doit être assurée par les gestionnaires de centres et d'enseignes commerciaux.

Les salariés doivent avoir été sensibilisés aux comportements à adopter en cas de situation suspecte, de menace d'attaque terroriste, de confinement ou d'évacuation. Ils doivent également avoir été informés de la procédure de signalement des comportements suspects en vigueur dans leur établissement. Par ailleurs, les responsables d'enseignes sont incités à former leur personnel aux gestes de premiers secours.

La connaissance fine des sites par le personnel qui y travaille et l'organisation d'exercices collectifs constituent des prérequis indispensables.

- *Le renforcement des échanges et de la coordination entre acteurs publics et privés :*

Ce renforcement se matérialise par la mise en place ou l'adaptation de conventions locales de coopération de sécurité.

Pour rappel, la convention nationale, signée le 19 février 2019, entre le secrétaire d'Etat auprès du ministère de l'Intérieur et les principales organisations professionnelles représentant les grandes surfaces commerciales promeut des conventions locales « visant au développement d'un plan de sécurisation suivi et pérenne des espaces commerciaux ». Il est recommandé à ces établissements de mettre en place un plan de sûreté et de désigner un coordonnateur en gestion de crise.

Ces types de coopération animés dans le cadre de la police de sécurité du quotidien (PSQ) instaurent une confiance mutuelle et impulsent une nouvelle dynamique d'échanges d'informations. Le développement de ces conventions locales est recherché.

- *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 :*

Les responsables de la sécurité du secteur marchand privilégient la surveillance dynamique des espaces, la détection des comportements suspects et le recours à la 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 les lieux susceptibles d'être exposés à des actes de terrorisme (Cf. art. L. 223-1 du code de la sécurité intérieure).

Il est souhaitable que les préfets accordent aux espaces de commerce, dans toute la mesure du possible, l'extension de leur vidéosurveillance aux abords immédiats de la voie publique.

De même, les préfets examinent les demandes des espaces de commerce d'autoriser, à titre exceptionnel, la présence d'agents privés de sécurité, même itinérants, sur la voie publique, aux abords de leur site.

4.3 Sécurité des transports collectifs

- *Contexte général*

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.). A ces occasions, le niveau de sécurité des plateformes aéroportuaires, des gares, des ports et des réseaux de transport en commun doit être renforcé[3].

- *Objectifs de sécurité recherchés sur la période*
  - *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.

  - *Spécificité du transport aérien*

Même si la pandémie impacte la fréquentation 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'Etat et les opérateurs poursuivront l'amélioration de la sécurisation du côté ville.

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

  - *Infrastructures et réseaux ferroviaires*

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 ;
  - **mèl** : permanence.cmvoa@developpement-durable.gouv.fr

- *Transport maritime de passagers*

Il est recommandé aux exploitants portuaires et aux armateurs d'assurer la continuité du contrôle des véhicules, de leurs passagers et de leur chargement. Conformément à l'arrêté du 16 juillet 2018, modifiant l'arrêté du 4 juin 2008[4], 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. A ce titre, tout armateur exploitant des navires rouliers à passagers mettra 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.

L'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.), est reconduit.

Sous l'autorité des préfets maritimes, le déploiement aléatoire d'équipes de protection constituées d'agents de l'Etat, à bord des navires à passagers sous pavillon français à destination des îles métropolitaines, dont notamment la Corse, ainsi qu'à destination du Royaume-Uni reste en vigueur. En cas de menace avérée, le déploiement de ces agents est également possible à bord des navires à passagers sous pavillon français à destination de l'Algérie et de la Tunisie.

---

[3] L'efficacité des mesures de contrôle dans les transports peut être accrue par le rappel des dispositions tirées des lois SAVARY, URVOAS et LEROY de 2016.

[4] En application de cet arrêté modificatif, la fiche MAR 10-03 a été créée et ajoutée au plan gouvernemental VIGIPIRATE.

Afin de protéger le trafic maritime d'intérêt, l'incitation à adhérer à la coopération navale volontaire doit être poursuivie, auprès des armateurs français et étrangers, comme auprès des opérateurs terrestres qui font appel à des services maritimes.

Conformément à la mesure MAR 12-02, l'application du niveau 2 du code ISPS est maintenue dans les zones suivantes : au Nord-ouest de l'Océan indien, dans le Golfe arabo-persique, dans la zone comprise entre les mers de Sulu et Célèbes (espace compris entre le nord de l'Indonésie et les Philippines), dans le détroit de Malacca, dans le Golfe de Guinée et dans les ports de Libye. Par ailleurs, compte tenu du nombre d'incidents dans le détroit de Singapour, situé dans le prolongement du détroit de Malacca, le niveau ISPS 2 sera appliqué dans cette zone.

4.4 Sécurité des bâtiments publics

- *Contexte général et objectif de sécurité recherché sur la période*

Un effort particulier devra être porté sur la protection des sites préfectoraux et/ou interministériels situés hors du siège central de la préfecture de département ou de région.

Il convient d'actualiser les annuaires de crise au sortir de la période estivale et les procédures d'alerte afférentes de même que les plans de protection et les procédures internes d'évacuation ou de confinement seront portés à la connaissance des nouveaux arrivants.

Une vigilance particulière sera également portée aux bureaux de vote pendant la durée des élections mais aussi à la sécurité des palais de justice et des établissements pénitentiaires dans le contexte de procès dits « sensibles ». Elle 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.

Cette vigilance peut également concerner **les sites de la protection judiciaire de la jeunesse**, qui prend en charge des mineurs poursuivis pour association de malfaiteurs à but terroriste.

4.5 Sécurité des établissements scolaires, de l'enseignement supérieur et de l'enseignement technique agricole ainsi que des structures d'accueil collectif de mineurs (ACM) à caractère éducatif

- *Contexte général*

Dans le contexte actuel de menace terroriste élevée, l'attaque du 16 octobre 2020 visant un professeur a rappelé la sensibilité des services et les des établissements de rattachement des ministères de l'éducation nationale, de la jeunesse et des sports et de l'enseignement supérieur, de la recherche et de l'innovation (MENJS/MESRI). Pour autant, cela ne doit pas occulter la crise sanitaire actuelle ainsi que les autres types de risques et menaces (technologique, naturelle, cyberattaque…) auxquels les populations sont potentiellement exposées.

A ce titre, le ministère de l'éducation nationale, de la jeunesse et des sports, et le ministère de l'enseignement supérieur de la recherche et de l'innovation en relation avec leurs partenaires, en particulier les forces de sécurité intérieure, mettent en place toutes les mesures jugées nécessaires afin de sécuriser les personnels et les biens relevant de leurs ministères et ainsi apporter une réponse adaptée.

C'est ainsi que les services et les établissements des MENJS/MESRI prendront les dispositions visant à se prémunir contre les menaces identifiées en participant activement à la mise en œuvre opérationnelle des politiques publiques en matière de protection des populations, en s'appuyant sur les directives interministérielles[5]. La complémentarité des actions au sein de l'appareil de gestion de crise décliné à l'échelon territorial est fondamentale, et sera systématiquement privilégiée.

[5] Instruction relative au renforcement des mesures de sécurité et de gestion de crise applicables dans les écoles et les établissements scolaires du 12 avril 2017 et télégramme interministériel du 28 août 2020 relative à la protection de l'espace scolaire – bilan de l'année 2019-2020 et préparation de la rentrée scolaire 2020-2021

- *Objectifs de sécurité recherchés sur la période en réponse immédiate à l'attentat perpétré le 16 octobre 2020 :*
    - Mise à disposition d'un dispositif national d'écoute et de soutien psychologique pour tous les personnels de l'Education nationale : 0 805 500 005 (numéro d'appel joignable 24h/24, 7 jours/7)
    - Identification des situations susceptibles de faire peser une menace sur les personnels et/ou les infrastructures, comportant un ou des risque(s) supposé(s) ou identifié(s).
    - En complément de l'identification des situations évoquées ci-dessus, procéder au renforcement de la sécurité des personnels et biens, impactés directement par l'attentat du 16 octobre 2020 :
        - Renforcement des mesures de sécurité des personnels logés au sein des écoles et établissements scolaires.
        - Renforcement des mesures de sécurité des enseignants intervenant en milieu pénitentiaire.
        - Renforcement des mesures de sécurité des personnels effectuant des contrôles d'instruction en famille.
        - Renforcement des mesures de sécurisation des emprises bâtimentaires des services de l'administration centrale et territoriale des MENJS/MESRI ainsi que des établissements scolaires.
    - La mise en œuvre d'actions additionnelles visant le renforcement de la sécurité des personnels et des biens, notamment :
        - Une circulaire MININT/MENJS en cours d'élaboration afin de décliner les actions opérationnelles conjointes jugées nécessaires dans ce contexte spécifique.
        - Des instructions spécifiques aux équipes mobiles de sécurité (EMS) académiques ayant la charge de garantir la sécurité et la protection des établissements scolaires.
    - Les mesures mises en œuvre pour la rentrée scolaire à la date du 2 novembre, suite aux vacances de la Toussaint :
        - Des actions coordonnées dans les territoires entre les services de l'Education nationale et les services des autres secteurs ministériels, dont les forces de sécurité intérieure, afin de sécuriser au mieux la rentrée scolaire du 2 novembre, les manifestations et rassemblements se rapportant à l'attentat et à ses suites.
- *Objectifs de sécurité recherchés sur la période au regard de la crise sanitaire actuelle :*
    - Reconduction des principales mesures Vigipirate

Compte tenu des préconisations actuelles liées à la crise sanitaire, les procédures d'accès et d'organisation des activités des services et établissements du MENJS/MESRI ont été aménagées (port du masque, distanciation physique, limitation du brassage de la population, …).

Ces consignes ne doivent cependant 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 celles organisées par les structures d'accueil collectif de mineurs.

Dans cette perspective, l'obligation généralisée du port du masque constitue certes une nécessité sanitaire mais peut s'avérer être une complexité supplémentaire en terme de contrôle visuel.

Cependant, malgré cela, il est impératif de maintenir une surveillance active et un contrôle pertinent des accès aux différentes emprises bâtimentaires.

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

Dans certains établissements ou opérateurs sous tutelle MENJS/MESRI/MAA, une attention particulière sera portée à la protection et aux contrôles des lieux abritant des matériels et des produits toxiques. De manière générale, les zones considérées comme « sensibles », (zones à régime restrictif, zones sécurisées, zones d'accès restreint…), doivent faire l'objet d'une vigilance maximale et de la mise en place de procédures de contrôle renforcées.

- Sécurisation des personnes et des biens, plan de continuité/reprise d'activité

Il est nécessaire de poursuivre l'élaboration et/ou la mise en œuvre des plans de continuité et des dispositifs de gestion de crise. En outre, l'élaboration et/ou la mise à jour des diagnostics de sécurité, de sûreté et des PPMS « attentat-intrusion », ainsi que la réalisation des exercices annuels associés doivent être menés à bien.

Pour les ACM : renforcer la surveillance des accès aux accueils (accueils de loisirs, séjours de vacances et camps scouts) et mettre en œuvre les bonnes pratiques de prévention figurant dans le « guide à destination des organisateurs, des directeurs et des animateurs en charge d'accueils collectifs de mineurs à caractère éducatif ».

- Sécurisation des systèmes d'information (données et infrastructures physiques)

Il est demandé aux services et établissements des MENJS/MESRI de veiller à :

- la protection à un niveau adéquat des locaux dédiés à l'installation des systèmes d'information, des stockages de données et des systèmes de restauration,
- l'utilisation de systèmes d'information présentant un niveau de sécurité compatible avec la note ministérielle HFDS N°2020-0363 du 21/07/2020 relative aux « modalités de souscription à des offres de services d'informatique en nuage », le guide d'hygiène informatique de l' agence nationale de la sécurité des systèmes d'information, ainsi que les dispositions relatives au règlement général sur la protection des données (RGPD) en visant notamment la protection des données personnelles,
- le respect de la politique de sécurité des systèmes d'information (PSSIE) afin de satisfaire aux exigences de cyber sécurité.

Enfin la crise sanitaire a modifié sensiblement l'organisation du travail. A cet égard, l'activité en télétravail doit prendre en considération le risque cyber et c'est pour cette raison que la politique de sécurisation des systèmes d'information (PSSI) doit être considérée prioritaire à tous les échelons de nos organisations, y compris au plan local, dans sa déclinaison au plus près des agents.

- Collaboration étroite entre les acteurs de la gestion de crise au plan local

Afin de contribuer pleinement à l'action coordonnée de l'ensemble des administrations dans les territoires, au regard des problématiques de sûreté, de sécurité, et plus encore, d'anticipation et de gestion de crise, une approche partenariale visant à renforcer les mesures de protection des personnes et des biens, tout en développant une culture partagée de la sûreté et de la sécurité, doit guider ces actions telles que déclinées par la circulaire interministérielle du 12 avril 2017 relative au renforcement des mesures de sécurité et de gestion de crise applicables dans les écoles et les établissements scolaires. Le partage d'informations entre les différents acteurs doit se traduire concrètement par :

- la participation des différents acteurs aux projets de sécurisation des services et établissements,
- le déploiement de procédures partagées des chaines d'alerte et de gestion de crise,
- la mise à jour des annuaires interministériels des acteurs de la gestion de crise et communication des PPMS « attentat-intrusion » et des plans bâtimentaires,

- la mise en œuvre d'exercices communs.

Les points énumérés ci-dessus n'excluent en rien les autres actions qui peuvent être entreprises dans ce même esprit, y compris en élargissant cette posture à d'autres secteurs ministériels. Ces derniers ont d'ailleurs toute latitude pour se nourrir des réflexions du MENJS/MESRI/MAA.

4.6 Sécurisation des sites touristiques, culturels et des expositions à thème sensible

➢ *Contexte général*

Malgré le ralentissement de la fréquentation des sites et événements culturels lié à la situation sanitaire, la vigilance face au risque terroriste ne doit pas faiblir.

➢ *Préconisations*

Les recommandations portent principalement sur la protection des abords des sites culturels en raison de la fréquentation habituelle de ces espaces et de leur exposition particulière à la menace terroriste.

Les exploitants et propriétaires sont invités à veiller tout particulièrement à sécuriser les files d'attente. De même, pour le spectacle vivant, l'attention portée aux entrées et aux sorties des spectacles et rassemblements doit être maintenue.

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.

D'une manière générale, il est recommandé d'entretenir des relations régulières avec les forces locales de police et de gendarmerie.

Plusieurs documents élaborés pour soutenir les responsables de sites ou d'événements peuvent être consultés sur le site Internet du ministère de la Culture :

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

Cette documentation doit permettre la réalisation d'exercices dans la perspective de valider les procédures internes de confinement ou d'évacuation en cas d'attaque directe ou à proximité.

➢ *Sauvegarde des biens culturels*

Compte tenu des sinistres récents, les établissements culturels sont invités à compléter ou à mettre à jour leur plan de sauvegarde des biens culturels (PSBC). La protection du patrimoine culturel compte parmi les objectifs du dispositif ORSEC, le PSBC doit donc être réalisé en relation étroite avec les services de secours et être mis à leur disposition en cas d'intervention.

4.7 Sécurité des établissements de santé, sociaux et médico-sociaux

➢ *Contexte général*

Les établissements de santé, sociaux et médico-sociaux, par nature ouverts sur l'extérieur, demeurent des cibles particulièrement vulnérables. La vigilance doit donc rester élevée particulièrement pour les établissements de santé, médico-sociaux et pour les sites de production, de stockage et de distribution de produits de santé (masques, EPI..).

➢ *Objectifs de sécurité recherchés sur la période*

Les préfectures veillent au maintien des actions mises en œuvre par les forces de sécurité intérieure :

- la sécurisation des abords des établissements de santé de niveau 1 (selon la cartographie transmise par les ARS) ;
- le renforcement immédiat, en cas d'attentat, des établissements accueillant des victimes, afin de prévenir les risques de sur-attentat.

Les directeurs d'établissement de santé s'assurent de l'effectivité de la mise en œuvre des mesures de sûreté de leur plan de sécurisation d'établissement (PSE). Ils poursuivent les actions de formation à destination de leurs personnels et s'attachent à s'assurer de leur efficacité.

Les responsables des établissements et des services sociaux et médico-sociaux (ESSMS), poursuivent le déploiement de leur stratégie de protection, en suivant les recommandations du ministère des solidarités et de la santé.

Point d'attention :

- la sécurisation des centres de prélèvement ou de vaccination ;
- les opérateurs d'importance vitale doivent faire l'objet d'une vigilance toute particulière au regard de la crise sanitaire actuelle. Les sites de production de médicaments (vaccins, hydroxychloroquine) méritent également la mise en œuvre de mesures de sécurisation adaptées.

4.8 Protection des ressortissants et intérêts français à l'étranger (IFE)

- *Contexte général*

A l'étranger, la France peut être directement menacée par des organisations terroristes.

La circulaire du Premier ministre n°5777/SG du 26 mars 2015 définit le rôle capital de l'Ambassadeur pour assurer la sécurité des agents et des implantations de la France à l'étranger.

L'augmentation de la menace terroriste pouvant viser directement les agents de l'Etat et des opérateurs du MEAE à l'étranger, ainsi que les implantations étatiques françaises est prise en compte.

Cette évaluation de la menace définit également les mesures à prendre pour assurer la sécurité de la communauté française et des touristes français.

- *Objectifs de sécurité recherchés et acteurs concernés*

L'Ambassadeur avec l'appui des responsables des services de l'Etat et des opérateurs procède à une analyse des risques potentiels et propose une stratégie de sécurité qui porte à la fois sur les actions à mettre en place et les mesures préconisées pour le renforcement de la sécurité des agents et des implantations.

Les actions et mesures de protection des ressortissants français, résidents ou de passage à l'étranger suivent trois axes :

- *Information et sensibilisation*

Edition des « *Conseils aux voyageurs* », régulièrement mise à jour.

Recommandations sur les déplacements dans les zones « *déconseillées sauf raison impérative* » et « *formellement déconseillées* » et, au besoin, incitation à renoncer au déplacement.

Conseil aux entreprises, opérateurs et ONG dans ces zones.

Envoi de message d'alerte en temps réel en cas de risque d'enlèvement ou d'attentat.

Réponse téléphonique active (24/7).

- *Formation des agents des postes diplomatiques et consulaires à la gestion de crise et aux accidents collectifs*
- *Assistance aux victimes françaises en cas d'attaque terroriste à l'étranger*

Mise en œuvre d'une cellule de crise, dans les ambassades ou à Paris.

Elaboration de plans d'urgence destinés à organiser la prise en charge de victimes françaises.

Suivi des familles de victimes d'actes terroristes et de prises d'otages à l'étranger.

Les actions de protection des implantations françaises à l'étranger et des agents de l'Etat portent sur les mesures de sécurité active et passive ainsi qu'organisationnelles. Elles incluent des volets de formation renforcée, notamment des exercices de confinement/évacuation, de formation « *Comment réagir à la réaction en cas d'attaque armée* » et de formations longues « *Départ en postes sensibles* ».

4.9 Sécurité du numérique (ANSSI)

- *Contexte général*

Les menaces visant les administrations et les entreprises privées restent élevées et variées (attaques par rançongiciels, attaques indirectes et vulnérabilités critiques).

➢ *Objectifs de sécurité recherchés sur la période*

- Mesure NUM 31-09 Rappeler l'importance d'une mesure d'hygiène ou sectorielle existante :
    - Pour la sécurisation des accès à distance des systèmes d'information, recourir à une authentification forte, par exemple avec un mot de passe et un certificat stocké sur un support externe (carte à puce ou jeton USB) ou un mécanisme de mot de passe à usage unique (*One Time Password*), afin d'éviter toute réutilisation d'authentifiants depuis un poste volé ou perdu et s'assurer du caractère sécurisé de la connexion réseau à travers Internet lorsqu'un utilisateur a besoin de se connecter au système d'information de l'entité à distance.
    - Au regard de la menace *Emotet*, sensibiliser les utilisateurs à ne pas activer les macros dans les pièces jointes et à être particulièrement attentifs aux courriels qu'ils reçoivent et réduire l'exécution des macros selon la technique de l'hameçonnage (rappel sur la fiche hameçonnage : http://www.sgdsn.gouv.fr/vigipirate/securite-du-numerique-lhameconnage-ou-phishing/)
- Concernant les vulnérabilités critiques (NUM 41.01), les opérateurs et administrations doivent appliquer les correctifs de sécurité mentionnés dans l'annexe des mesures correspondant à cinq bulletins d'alerte du CERT-FR disponibles sur le site www.cert.ssi.gouv.fr.
- Compte tenu de la menace persistante liée aux rançongiciels, les opérateurs et les administrations s'assurent que le plan de continuité d'activité (PCA) est opérationnel et que le personnel chargé de le mettre en œuvre est familiarisé avec celui-ci. Il est par ailleurs recommandé d'effectuer un exercice d'activation du PCA si le dernier exercice a été effectué il y a plus d'un an (NUM 51-02).

Les opérateurs et les administrations doivent également être en capacité de restaurer le bon fonctionnement de leurs systèmes les plus critiques en cas de destruction ou d'altération des données par un rançongiciel en s'assurant que les éléments sauvegardés ne soient pas accessibles par un quelconque réseau, y compris avec des comptes d'administration (NUM 51-06). Face à cette menace persistante et grandissante, l'ANSSI a sorti un guide en septembre 2020 *Attaques par rançongiciels, tous concernés. Comment les anticiper et réagir en cas d'incident ?*[6]

[6] https://www.ssi.gouv.fr/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/

5 Consignes particulières de vigilance, prévention et protection

5.1 Sensibilisation des personnels 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 seront sensibilisées et informées par leurs autorités de tutelle des mesures de sécurité à appliquer.

5.2 Sensibilisation à la menace des attaques par véhicules-béliers

Les attaques par véhicules-béliers demeurent un mode d'action fréquemment utilisé par les 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 : http://www.sgdsn.gouv.fr/vigipirate ;
- le guide du ministère de l'intérieur évoqué au § 4.1.

5.3 Vigilance et mesures de prévention face au risque NRBC-E (nucléaire, radiologique, biologique, chimique, explosif).

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

/pixaf@gendarmerie.interieur.gouv.fr – 01 78 47 34 29 (24/7).

5.4 [DR]

5.5 Sensibilisation à la lutte anti-drone

L'utilisation des drones est un mode d'action régulièrement mis en œuvre pour capter des images ou diffuser des messages[7] mais qui peut évoluer vers des actes de malveillance ou terroristes. A l'occasion de grands rassemblements, les organisateurs doivent prendre en compte cette menace en sollicitant l'avis des référents sûreté locaux de la police ou de la gendarmerie nationales.

6 Sensibilisation du grand public

Malgré la crise sanitaire actuelle, le niveau élevé de la menace exige le maintien d'une vigilance accrue.Efforts de communication

Les ministères veilleront à ce que les opérateurs publics et privés situés dans leur champ de compétence mettent en place les logogrammes **: « *Sécurité renforcée - risque attentat* ».**

Ces logogrammes peuvent être téléchargés sur le site :

- du Gouvernement http://www.gouvernement.fr/vigipirate ;
- du SGDSN http://www.sgdsn.gouv.fr/vigipirate .

Les ministères et les préfets sont invités à relayer le plus largement possible les outils de sensibilisation à la menace terroriste téléchargeables sur les deux sites cités *supra*.

[7] Comme lors d'un match de football au Luxembourg le 3 octobre 2019.

6.2 Sensibilisation des professionnels et du grand public aux bonnes pratiques

Dans un souci de large diffusion des bonnes pratiques face à la menace terroriste, figurent en annexe des fiches de sensibilisation à destination, tant du grand public que des professionnels. Ces fiches renouvelées sont accessibles en ligne depuis l'espace Vigipirate du site Internet du SGDSN.

Elles sont également sur l'espace dédié du site du Gouvernement : http://www.gouvernement.fr/risques/le-citoyen-au-coeur-du-nouveau-dispositif-vigipirate.

La communication des mesures et des comportements à adopter en cas d'attaque terroriste au sein des établissements et lieux recevant du public doit être renforcée. Elle peut se faire par le biais de l'affiche « *Réagir en cas d'attaque terroriste* ». Cette affiche, qui peut être téléchargée sur le site du gouvernement (http://www.gouvernement.fr/reagir-attaque-terroriste), ainsi que sur le site du SGDSN, doit être imprimée sur un format adapté au lieu où elle est placée et visible du public (privilégier les entrées et sorties des établissements, les halls, ou salles d'attente, etc.).

En complément de ce dispositif, le *service d'information du gouvernement* (SIG) vient de diffuser une affichette intitulée « *Les gestes d'urgence si quelqu'un a été blessé autour de vous* ». Elle délivre des messages simples et concis pour expliquer comment faire un garrot, comment faire cesser les saignements, ou encore comment prendre en charge une personne ayant perdu connaissance, en attendant l'arrivée des secours.

L'affichette est diffusée sur les réseaux sociaux et peut-être téléchargée sur : http://www.gouvernement.fr/reagir-attaque-terroriste.

Par ailleurs, un ensemble de guides de bonnes pratiques, à destination des professionnels et des particuliers, est mis à disposition sur les deux sites précédemment cités.

La version publique du plan Vigipirate « *Faire Face Ensemble* », également disponible en langue anglaise, peut y être téléchargée.

Enfin, le SGDSN a développé, en liaison avec de nombreux partenaires, une plateforme de sensibilisation VIGIPIRATE qui se veut un outil pédagogique accessible au plus grand nombre.

Cette plateforme s'appuie en particulier sur le document « *Faire Face Ensemble* » de 2016 mais aussi sur les guides de bonnes pratiques destinés aux professionnels.

Elle intègre 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.

Elle permet, 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.

Ce site internet a été mis en ligne le 20 septembre 2019 à l'adresse www.vigipirate.gouv.fr.

ANNEXES

Annexe 1 : Cartographie des attentats aboutis , échoués, déjoués en Europe de 2019 au 16 octobre 2020.
Diffusion sans restriction.

Annexe 2 : Historique des attentats aboutis, échoués, déjoués en France de 2015 au 16 octobre 2020
Diffusion sans restriction.

Annexe 3 : Fiche pratique Hameçonnage.
Diffusion sans restriction.

Annexe 4 : Fiche pratique chaine d'alerte en cas de menace.
Fiche à destination des responsables sûreté des établissements recevant du public

Annexe 5 : Fiche pratique prévention et signalement des cas de radicalisation djihadiste.
Diffusion sans restriction.