MINISTÈRES
SOCIAUX

Liberté
Égalité
Fraternité

Secrétariat général

Haut fonctionnaire
de défense et de sécurité

Paris, le 23 octobre 2020

Affaire suivie par : Matthieu Pianezze
Courriel : HFDS@sg.social.gouv.fr
Tél. : 01 40 56 48 49
HFDS/2020/38

NOTE

à l'attention de

MESDAMES ET MESSIEURS LES CONSEILLERS DE DEFENSE ET DE SECURITE DE ZONE,
LES DELEGUES DE DEFENSE ET DE SECURITE,
LES OFFICIERS ET RESPONSABLES DE SECURITE

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

Réf. :
Partie publique du plan gouvernemental de vigilance, de prévention et de protection face aux menaces d'actions terroristes n°102000/SGDSN/PSN/PSE du 1er décembre 2016 ;
Instruction N°SG/HFDS/PDS/2018/54 du 31 janvier 2018 relative à la mise en œuvre du plan Vigipirate au sein des périmètres des ministères sociaux.
PJ. : Annexe relative au « Tableau des mesures de vigilance ».

Le niveau de vigilance « sécurité renforcée-risque attentat »
est maintenu sur l'ensemble du territoire national.

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 crise sanitaire générée par la pandémie de COVID-19, la menace terroriste reste à un niveau élevé.

Cette posture Vigipirate adapte 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, écoles et universités), **avec une attention particulière sur les établissements de santé, médico-sociaux et sociaux, ainsi que la sécurité des sites de production, de stockage et de distribution des produits de santé**.

Le contexte particulier de la crise COVID rend impossible d'établir sur la période 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.

I. Évaluation des menaces

Menace terroriste

A ce jour**, 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 menace reste principalement portée par **des individus endogènes**.

A l'étranger, la capacité de projection de l'*Etat Islamique* (EI) est réduite en raison de son retour à la clandestinité en zone syro-irakienne. **Son objectif principal à ce jour est d'inspirer des acteurs endogènes au moyen de sa propagande**.

Sur le territoire national, la menace djihadiste se traduit principalement par le passage à l'acte de sympathisants, parmi lesquels on compte encore des djihadistes frustrés après un projet de départ entravé vers la zone syro-irakienne, ainsi que des terroristes inspirés par l'EI mais n'ayant pas montré de velléités avant leur passage à l'acte. **Ces individus nourrissent le caractère imprévisible de la menace**.

Dans ce contexte général, comme l'illustre l'attaque parisienne du 25 septembre lié à la republication des caricatures de Mahomet par le journal satirique Charlie Hebdo ou les débats sur la liberté d'expression à la suite de l'assassinat du professeur d'histoire-géographie Samuel Paty, ainsi que la tenue de procès d'affaires terroristes médiatisées, **accroissent le risque de passage à l'acte.**

Par ailleurs, les mouvances contestataires « *ultras* » instrumentalisant de potentielles tensions sociales pourraient s'agréger aux manifestants, afin de se livrer à des violences.

Menace cyber

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, établissements de santé, …) que des entreprises privées (ex : énergie, santé, aéronautique, …). L'épidémie COVID-19 a donné lieu à une recrudescence de ce type d'attaques, notamment par le biais de courriels sur le thème de la crise sanitaire, proposant des liens ou des pièces jointes malveillantes.

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* [1] *?*

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

Depuis le déclenchement de la crise liée à la 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, et augmenté la surface potentielle d'attaque.

Les opérateurs et les administrations doivent porter une attention particulière aux systèmes d'information, notamment ceux liés à la gestion de la crise COVID-19, et être en capacité de restaurer le bon fonctionnement de leurs systèmes les plus critiques en cas de destruction ou d'altération des données. La viabilité des sauvegardes est primordiale, les éléments nécessaires à la restauration des environnements et des données doivent être sanctuarisés (Segmentation réseau, revue des comptes nécessaires aux opérations, revue des droits associés).

L'ANSSI constate actuellement un ciblage d'entreprises et d'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, comme le code répertorié sous le nom de TrickBot. La détection et le traitement au plus tôt des évènements de sécurité lié à Emotet et TrickBot peut prévenir de nombreux types d'attaques, dont celles par rançongiciel avant le chiffrement.

II. Adaptations de la posture Vigipirate pour les ministères sociaux

Il est demandé aux organismes publics ou privés relevant du champ de compétences des ministères sociaux de **poursuivre la mise en œuvre des mesures figurant en annexe**, tout en tenant compte des dispositions prises dans le décret n°2020-1257 du 14 octobre 2020 prescrivant les mesures générales nécessaires pour faire face à l'épidémie de COVID-19 dans le cadre de l'état d'urgence sanitaire**.**

Dans le contexte de la gestion de la crise COVID-19, **une vigilance toute particulière** est à porter, **en lien constant avec les forces de sécurité intérieure (FSI)** sur :

- Les opérateurs d'importance vitale ;
- La sécurisation du matériel médical et des locaux abritant des équipements de protection individuels (EPI) des établissements de santé support des groupements hospitaliers de territoire (GHT) ;
- Les centres de prélèvement ou de vaccination ;
- Les sites de production de médicaments (vaccins, hydroxy chloroquine, …) ;
- Les lieux de stockage des futurs vaccins contre la COVID-19, qui au regard de leur grande sensibilité feront l'objet d'un dispositif adapté.

Vous veillerez à diffuser cette prolongation de posture à l'ensemble des correspondants de vos secteurs d'activités respectifs et de faire remonter au service spécialisé du HFDS des ministères sociaux les points d'attention et les difficultés rencontrées dans son application (hfds@sg.social.gouv.fr).

Le haut fonctionnaire adjoint
de défense et de sécurité
Général (2s) Arnaud Martin

ORIGINAL SIGNE

ANNEXE

PROLONGATION DE LA POSTURE « AUTOMNE HIVER 2020 – PRINTEMPS 2021 »

RAPPEL DES MESURES SOCLES ET ADDITIONNELLES EN VIGUEUR

TABLEAU DES MESURES DE VIGILANCE (1/5)[2]

Action	Libellé des principales mesures	Commentaires	N° mesure
ALERTE ET MOBILISATION (ALR)	Disposer d'une chaine d'alerte et d'information la plus large possible, la vérifier et la tester régulièrement. Diffuser l'alerte au grand public. Rappeler les conduites à tenir en réponse à la menace d'actions terroristes (colis abandonné, alerte à la bombe, fusillade,…). Elaborer et mettre à jour un plan de continuité d'activité (PCA).	- Afficher le logo du niveau **« *sécurité renforcée-risque attentat* »** à l'entrée des sites accueillant du public.  Ces logos doivent être visibles à l'entrée et dans les espaces d'attentes des sites accueillant du public et peuvent être complétés d'une fiche synthétique récapitulant les conditions particulières de sécurité au sein de la structure. Il convient d'actualiser régulièrement les annuaires de crise, de sensibiliser les agents aux procédures d'alerte et d'organiser des exercices simples sur ces thématiques.	ALR 10-01 ALR 11-02 ALR 11-04 ALR 20-01
RASSEMBLEMENT ET ZONES OUVERTES AU PUBLIC (RSB)	Renforcer la surveillance et le contrôle. Mettre en œuvre des dispositifs de protection pour faire face aux différents modes opératoires terroristes. Procéder à des contrôles d'identité, visite de véhicules, inspection et fouille de bagages dans les lieux identifiés.	En local, et en lien constant avec l'évolution de la situation liée à l'épidémie de COVID-19, un contact avec les forces de sécurité intérieure est recommandé afin d'aider les organisateurs dans leur appréciation du risque. Au regard de la menace associée aux attaques par véhicules-béliers les opérateurs sont encouragés à renforcer les dispositifs de protection passive (plots, barrières, blocs en béton, etc.) sur les accès les plus fréquentés.	RSB 11-01 RSB 12-01 RSB 13-01 RSB 12-05 RSB 20-02 RSB 20-03

[2] NB : Seules les principales mesures publiques intéressant les secteurs des ministères sociaux sont présentées dans cette annexe. La totalité des mesures est disponible dans le catalogue des fiches mesures VIGIPIRATE (CD).

TABLEAU DES MESURES DE VIGILANCE (SUITE 2/5)

Action	Libellé des principales mesures	Commentaires	N° mesure
INSTALLATIONS ET BATIMENTS (BAT)	Renforcer la surveillance et contrôler les abords des installations et bâtiments.	<u>Généralités :</u> Les mesures décrites sont applicables dans : - les établissements de santé, médico-sociaux et sociaux ; - les structures relevant de la protection de l'enfance ; - les établissements d'accueil du jeune enfant (EAJE) ; - les accueils collectifs de mineurs ; - les bâtiments publics (services publics, ministères).	BAT 10-01 BAT 10-02
	Surveiller et contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier).	Renforcement des échanges entre les responsables de sites et les forces de sécurité intérieure. Maintien du renforcement de la vigilance aux abords et des contrôles aux accès des établissements. Les mesures de contrôle peuvent notamment consister en des dispositifs de filtrage et d'inspection visuelle des sacs.	BAT 10-03 BAT 11-02 BAT 12-02 BAT 13-02 BAT 11-03 BAT 12-03
	Identifier les zones internes en fonction de leur sensibilité et en réglementer l'accès.	Sensibilisation à la détection et au signalement de comportements suspects, notamment auprès du personnel d'accueil.	BAT 20-01 BAT 21-01 BAT 22-01 BAT 23-01
	Renforcer la surveillance interne et limiter les flux (dont interdiction de zone).	Renforcement de la vigilance dans les domaines de la sécurisation des espaces de rassemblement (périphérie, périmétrie, intérieur).	BAT 30-01 BAT 30-02
	Mettre en œuvre des dispositifs de protection pour faire face aux différents modes opératoires terroristes (armes, explosif, véhicule bélier, etc.).	Etablissements d'accueil du jeune enfant (EAJE) et établissements relevant de la protection de l'enfance : Mise en œuvre des mesures préconisées dans la circulaire ministérielle n°DGCS/SD2C /2016/261 du 17 août 2016, notamment celles qui portent sur : - les moyens de protection et le protocole de mise en sûreté des enfants et du personnel ; - la formation du personnel et l'information des familles.	BAT 30-04 BAT 31-01 BAT 32-02

TABLEAU DES MESURES DE VIGILANCE (SUITE 3/5)

Action	Libellé des principales mesures	Commentaires	N° mesure
INSTALLATIONS DANGEREUSES ET MATIERES DANGEREUSES (IMD)	Restreindre l'accès du grand public aux précurseurs d'explosifs. Tenir à jour les inventaires des stocks de matières dangereuses pour détecter rapidement les vols ou disparitions et signaler ces disparitions aux autorités.	Une vigilance particulière sur les matières NRBC-E (précurseurs d'explosifs, acide sulfurique, bouteilles de gaz, etc.) est à exercer. Une fiche de recommandations pratiques, dédiée aux précurseurs d'explosifs est disponible sur le site Internet du SGDSN (http://www.sgdsn.gouv.fr/vigipirate). Signaler tous vols, disparitions ou transactions suspectes de précurseurs d'explosifs et agents NRBC au point de contact national : - pôle judiciaire de la gendarmerie nationale : pixaf@gendarmerie.interieur.gouv.fr Tél H/24 : 01.78.47.34.29. et au service spécialisé du HFDS : hfds@sg.social.gouv.fr	IMD 10-01 IMD 10-02 IMD 10-03 IMD 10-05 IMD 10-06 IMD 10-07 IMD 10-08 IMD 20-01
SECURITE DU NUMERIQUE (NUM)	Renforcer le niveau de sécurité des systèmes d'information liés à la gestion de la crise COVID-19. Renforcer la protection contre les intrusions dans les systèmes d'information. Renforcer la protection contre les attaques en déni de service. Alerter des incidents sur les systèmes d'information.	Une vigilance constante est à porter sur les systèmes d'information, notamment avec le recours massif au travail à distance, la mise en service de nouveaux moyens de connexion à distance et des SI liés à la gestion de la crise COVID-19. L'application des mesures NUM doit permettre de réduire les risques face aux menaces cyber. Effectuer des rappels réguliers sur les risques liés aux « messages piégés », qui constituent le premier vecteur d'infestation virale, notamment de « rançongiciels ». Appliquer les « mesures barrières » en cybersécurité : - sensibiliser l'ensemble des personnels à faire preuve de vigilance vis-à-vis des messages reçus ; - faire régulièrement des sauvegardes des données (ordinateurs, téléphone…) et en garder une copie déconnectée ; - appliquer les mises à jour de sécurité sur les équipements connectés (serveurs, ordinateurs, téléphones…) dès qu'elles sont disponibles ; - utiliser des mots de passe uniques et solides et activer la double authentification chaque fois que possible. En cas d'incident, alerter la chaîne de sécurité des systèmes d'information des ministères sociaux : - pour les établissements de santé, les établissements médico-sociaux, centre de radiothérapie et laboratoire de biologie sur le site de signalement des évènements sanitaires indésirables depuis l'espace dédié aux professionnels de santé : https://signalement.social-sante.gouv.fr - pour tous les établissements non indiqués ci-dessus à l'adresse : ssi@sg.social.gouv.fr.	NUM 51-02 NUM 52-02

TABLEAU DES MESURES DE VIGILANCE (SUITE 4/5)

Action	Libellé des principales mesures	Commentaires	N° mesure
SECTEUR SANTE (SAN)	Maintenir une capacité de veille sanitaire permanente. Pour les établissements de santé, maintenir une capacité de reprise et d'adaptation de l'offre de soins (prise en charge des victimes). Protéger les établissements de santé.	Les agences régionales de santé (ARS) veillent, d'une part, à bien articuler le schéma ORSAN AMAVI avec le plan ORSEC des préfectures et, d'autre part, à organiser le dispositif sanitaire des grands événements à sensibilité particulière selon les orientations des préfets. Les directeurs d'établissement de santé s'appuient sur leur plan de sécurisation d'établissement (PSE). Ce document est un outil essentiel sur lequel les établissements doivent pouvoir s'appuyer durant la gestion de la crise COVID-19. Les responsables des établissements et des services sociaux et médico-sociaux (ESSMS), poursuivent le déploiement de leur stratégie de protection, en s'appuyant sur les recommandations de l'instruction n°SG/HFDS/DGCS/2017/219 du 26 juillet 2017.	SAN 10-01 SAN 20-01 SAN 30-01 SAN 30-02 SAN 40-01
RESEAUX D'EAU (EAU)	Exercer la vigilance dans l'exploitation des réseaux d'eau.	Les opérateurs et les ARS établissent et mettent à jour l'évaluation des besoins en eau, en fonction des usages et des besoins prioritaires de la population et définissent le programme d'analyses périodiques de l'eau. L'arrestation en Sardaigne, fin novembre 2018, d'une personne soupçonnée de vouloir contaminer un réservoir d'eau, doit inciter à maintenir un haut niveau de vigilance, tout en veillant à l'opérabilité des différents plans afin d'éviter toute action malveillante, criminelles ou terroristes sur les réseaux d'eau. Le réseau de contacts avec les autorités doit être maintenu et mis à jour périodiquement. Les opérateurs sont prêts à mettre en œuvre les consignes de sur-chloration dans les délais impartis. A chaque livraison, les opérateurs contrôlent systématiquement la conformité des réactifs nécessaires au traitement de l'eau. Ils effectuent les études de vulnérabilité et des autodiagnostics. Les opérateurs portent à la connaissance des autorités tout incident pouvant avoir des conséquences sur la santé publique Les opérateurs et les ARS mettent en place une astreinte ou une permanence dans les laboratoires des exploitants et les laboratoires agréés en charge du contrôle sanitaire des eaux.	EAU 20-01 EAU 20-02 EAU 20-03 EAU 20-04 EAU 20-05 EAU 20-06 EAU 20-07 EAU 20-08 EAU 20-09 EAU 20-10 EAU 20-11 EAU 20-12 EAU 20-13

TABLEAU DES MESURES DE VIGILANCE (SUITE 5/5)

Action	Libellé des principales mesures	Commentaires	N° mesure
ETRANGER (EXT)	Avant tout déplacement à l'étranger : - consulter le site conseils aux voyageurs du MEAE. - s'inscrire sur Ariane (voyageurs). Site du MEAE : *https://www.diplomatie.gouv.fr*	Ces mesures de précaution permettent de : - recueillir les numéros utiles, prendre connaissance des consignes de sécurité et les conserver pendant toute la durée de leur séjour - recevoir des recommandations de sécurité par courriels si la situation le justifie ; - être contacté en cas de crise dans le pays de destination ; - prévenir, en cas de besoin, la personne contact désignée. Des mesures de restriction complémentaires ont été prises dans le cadre de l'état d'urgence sanitaire.	EXT 10-05 EXT 10-06

NB : Les mesures sont numérotées avec les critères suivants :

- trigramme de domaine :

ALR : Alerte	NUM : Sécurité du numérique
RSB : Rassemblements et zones ouvertes au public	SAN : Santé
BAT : Installations et bâtiments	EAU : réseaux d'eau
IMD : Installations et matières dangereuses	EXT : Etranger

- Numéro d'ordre (dans le tableau du plan Vigipirate) de la mesure de 01 à 0x pour les mesures du socle et de 01 à 0x pour les mesures additionnelles.
  Exemple : la mesure BAT 13-04 : est une mesure du secteur installations et bâtiments (BAT), s'inscrit dans le 1er objectif du secteur (adapter la sûreté externe).