Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

MINISTÈRE DE L'ACTION
ET DES COMPTES PUBLICS

SECRÉTARIAT GÉNÉRAL

SERVICE DU HAUT FONCTIONNAIRE DE DEFENSE ET DE SECURITE
TELEDOC 722
120 RUE DE BERCY
75572 PARIS CEDEX 12

Paris, le 29 AVR. 2019

N°SHFDS/2019/04/10826

NOTE POUR
MESDAMES ET MESSIEURS LES DIRECTEURS, OFFICIERS, DELEGUES ET RESPONSABLES DE SECURITE

Objet : Adaptation de posture VIGIPIRATE « Eté – Rentrée 2019 ».

Annexes :

1. Tableau des principales festivités et principaux événements organisés sur le territoire national touchant au domaine économique.
2. Infographie des attentats jihadistes réalisés, échoués, déjoués en France depuis 2015.
3. Cartographie des attentats jihadistes réalisés, échoués, déjoués en France et dans les pays limitrophes en 2018.
4. Fiche « *Journées européennes du patrimoine : comment sécuriser son établissement face à la menace terroriste ?* ».
5. Fiche « *Comment préparer ses déplacements et voyages à l'étranger ?* ».
6. Fiche « *Sécurité du numérique. Rançongiciel : vos données prises en otage* ».
7. Liste des différentes fiches pratiques VIGIPIRATE en vigueur.

La posture VIGIPIRATE « *Eté – Rentrée 2019* » est active à compter du 7 mai 2019. Elle s'applique, sauf événement particulier, jusqu'au 18 octobre 2019, veille des vacances de la Toussaint.

L'ensemble du territoire national est maintenu au niveau « *sécurité renforcée - risque attentat* ».

Dans un contexte de menace terroriste qui demeure à un niveau élevé, cette posture VIGIPIRATE doit permettre d'adapter le dispositif de sécurité nationale à la période estivale, ponctuée de nombreux rendez-vous, et d'anticiper la période de rentrées scolaire et universitaire. Dans ce cadre, elle met l'accent sur :

- la sécurité des sites touristiques et des grands rassemblements estivaux. Une attention particulière sera notamment portée sur les festivals, événements sportifs (championnats du monde féminin de football), commémorations (75e anniversaires du débarquement, fête nationale) ou sommets internationaux (G7 de Biarritz) ;
- la sécurité des transports collectifs de personnes, notamment au moment des principaux chassés croisés de l'été ;
- la sécurité des écoles, établissements scolaires et établissements d'enseignement supérieur et de recherche, notamment lors des journées de rentrée ;
- la sécurité des sites patrimoniaux, plus particulièrement lors des *Journées européennes du patrimoine.*

Enfin, cette posture rappelle les consignes :

- de vigilance à destination des représentants de l'autorité publique (militaires, policiers, gendarmes, surveillants pénitentiaires, douaniers, pompiers), à nouveau visés au cours des dernières semaines ;
- de protection des systèmes d'information face au risque d'attaques cybernétiques.

Après une description du contexte général et une évaluation de la menace, cette note de posture expose les objectifs de sécurité qui doivent être déclinés par les ministères.

Trois fiches de recommandations pratiques sont annexées 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, à l'instar des travaux réalisés suite à l'attentat de Strasbourg, le 11 décembre 2018.

La posture VIGIPIRATE « Eté - Rentrée 2019 » est active à compter du 7 mai 2019. Elle s'applique, sauf événement particulier, jusqu'au 18 octobre 2019.

L'ensemble du territoire national est maintenu au niveau « sécurité renforcée - risque attentat ».

SOMMAIRE

1. CONTEXTE GENERAL

1.1. Principaux événements sur le territoire national

La période couverte par la posture « Eté - Rentrée 2019 » s'applique, sauf événement particulier, jusqu'au 18 octobre 2019. Cette période est marquée par :

- les vacances estivales traditionnellement ponctuées par l'organisation de nombreux festivals sur l'ensemble du territoire national, ainsi que par des pics de fréquentation des moyens de transports, qu'ils soient aériens, maritimes, ferroviaires ou routiers ;
- les rentrées scolaires et universitaires qui correspondent également à une phase de reprise générale de l'activité sur l'ensemble du territoire national ;
- l'organisation des *Journées européennes du patrimoine* les 21 et 22 septembre 2019.

Cette période sera également marquée par plusieurs événements d'importance qu'il convient de prendre en considération :

- les élections européennes, le 26 mai 2019 ;
- le championnat du monde de football féminin du 7 juin au 7 juillet 2019. Neuf villes seront concernées : Montpellier, Nice, Valenciennes, Paris, Lyon, Reims, Le Havre, Grenoble, Rennes ;
- les 75e anniversaires des débarquements de Normandie (8 et 9 juin 2019) [1] et de Provence (13 au 16 août 2019) ;
- le sommet « *des deux rives* » à Marseille (23 et 24 juin 2019) ;
- le Sommet du G7 à Biarritz (25 au 27 août 2019)[2].

Ces événements requièrent une attention accrue des acteurs de la sécurité, qu'ils soient publics ou privés.

Le tableau en annexe 1 récapitule une partie des grands événements qui seront organisés sur le territoire national au cours de la période couverte par la présente posture. **Cette liste, non exhaustive, a vocation à être complétée au niveau local par les autorités préfectorales** qui restent juges du niveau de sûreté à atteindre pour encadrer les manifestations à forte affluence ou au caractère symbolique marqué. Ce tableau rappelle également les dates anniversaires d'événements liés au terrorisme, qui pourraient motiver un passage à l'acte de terroristes.

1.2. Prolongation des contrôles aux frontières intérieures

La France a rétabli les contrôles aux frontières intérieures le 13 novembre 2015. Ce rétablissement a, depuis, été régulièrement reconduit sur le fondement de l'article 25 du code frontières Schengen qui prévoit cette possibilité « *en cas de menace grave pour l'ordre public ou la sécurité intérieure d'un État membre* ». La réintroduction de ces contrôles devait expirer le 30 avril.

La France a informé la Commission européenne qu'elle prolongera ses contrôles aux frontières intérieures pour une durée de 6 mois dans la perspective du G7. Le dispositif actuel est donc maintenu jusqu'au 30 octobre 2019.

---

[1] Plusieurs événements sont organisés dans le cadre de ce 75e anniversaire du débarquement de Normandie. La cérémonie commémorative internationale aura lieu le 6 juin 2019.

[2] Six G7 thématiques seront organisés en amont du Sommet : 5-6 mai à Metz (environnement), 9-10 mai à Paris (égalité hommes – femmes), 16-17 mai à Paris (santé), 6-7 juin à Paris (social), 4-5 juillet à Paris (développement et éducation), 17-18 juillet à Chantilly (finances).

1.3. Elections européennes : mise en place d'un réseau européen de coopération électorale

Dans le cadre des prochaines élections européennes la Commission européenne a décidé de constituer un réseau européen de coopération électorale. Ce réseau est plus particulièrement destiné à assurer la protection contre les incidents de cybersécurité et la lutte contre les campagnes de désinformation.

Afin de constituer ce réseau, la Commission a invité les Etats membres à désigner un point de contact unique pour échanger avec ses homologues et faciliter les échanges d'expertises et de bonnes pratiques en particulier sur les vulnérabilités potentielles des dispositifs électoraux et les menaces auxquelles ils pourraient être confrontés.

1.4. Anticipation des conséquences liées au BREXIT

Le retrait du Royaume-Uni de l'Union européenne, avec ou sans accord, aura des répercussions à la frontière franco-britannique en termes de flux de transports de marchandises et de voyageurs.

Ces conséquences ont été anticipées par les administrations en charge des formalités et des contrôles frontaliers. Ainsi, la Douane, 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*", reposant sur l'anticipation et la dématérialisation des formalités douanières, a notamment été élaboré.

2. ADAPTATION DE LA POSTURE VIGIPIRATE « *ETE – RENTREE 2019* »

La posture VIGIPIRATE « *Eté-Rentrée 2019* » est active à partir du 7 mai 2019 et s'applique, sauf événement particulier, jusqu'au 18 octobre 2019. **L'ensemble du territoire national est maintenu au niveau « *sécurité renforcée - risque attentat* ».**

L'attention est appelée sur les axes d'efforts décrits ci-dessous. Il devra être veillé à leur bonne prise en compte et à leur large diffusion auprès des services et opérateurs situés dans leur périmètre de compétence.

2.1. Sécurité des grands espaces de commerce, de tourisme et de loisir

2.1.1 Contexte général

Les lieux de commerce, les espaces de loisirs et les sites touristiques majeurs restent des cibles privilégiées. Les interconnexions en milieu clos dotées de commerces (métros, gares, etc.) constituent également un point de vigilance.

Cette période estivale et de rentrée appelle une vigilance accrue notamment sur le secteur du tourisme et des parcs de loisirs. La sécurité est également renforcée autour des grands espaces de rassemblements ayant pour objet des activités commerciales ou artisanales ambulantes (salons d'expositions, foires, etc.). Enfin, la sécurité des grands espaces de commerce lors des soldes d'été, marquées par une forte affluence, demeure un axe d'attention majeur.

Les responsables de ces établissements recevant du public doivent porter leur effort sur le déploiement des mesures de sécurité appropriées.

2.1.2 Objectifs de sécurité recherchés sur la période

La sécurisation des grands espaces de commerce, des sites de loisirs et des personnes présentes (clients, visiteurs et personnels) passe, entre autres, par :

- *La sensibilisation des personnels :*

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

A ce titre, les salariés doivent être sensibilisés aux bons comportements à adopter en cas de situation suspecte, de menace d'attaque terroriste, de confinement ou d'évacuation. Ils doivent également être, entre autres, informés sur la procédure de signalement des comportements suspects en vigueur dans leur établissement.

Enfin, la connaissance du site par le personnel qui y travaille et l'organisation d'exercices collectifs constituent des prérequis indispensables afin de réagir de manière efficace et coordonnée en cas d'attaque. Par ailleurs, les responsables d'enseignes sont incités à former leur personnel aux gestes de premiers secours.

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

La capacité à faire face à une attaque terroriste dans les espaces de commerce et de loisirs passe par le renforcement des échanges d'informations entre les services de l'Etat et les responsables de la sûreté des opérateurs privés et publics. Ce renforcement se matérialise également par la mise en place ou l'adaptation de conventions locales de coopération de sécurité.

Le 19 février 2019, le secrétaire d'État auprès du ministre de l'intérieur et les principales organisations professionnelles représentant les grandes surfaces commerciales ont signé une convention nationale de partenariat destinée à apporter de nouvelles réponses aux problématiques de sûreté des grandes surfaces. Cette convention promeut la mise en place de 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. Ce dispositif doit permettre de mieux prendre en compte les nouvelles menaces.

Ces types de coopération s'inscrivent dans le cadre de la *police de sécurité du quotidien* (PSQ), en créant du lien, en instaurant la confiance chez les partenaires et en impulsant une nouvelle dynamique d'échanges et de partage d'informations. Les premières conventions ont été signées et les gestionnaires des espaces commerciaux sont encouragés à recourir à ce type de dispositif.

➢ *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, le recours à la vidéoprotection.

2.2. Sécurité des bâtiments publics (services publics et ministères)

Les travaux et les mesures destinés à rendre plus efficaces les interactions entre les responsables de sites et les forces de sécurité intérieure (FSI) conservent toute leur pertinence. Un effort sera porté sur les bâtiments publics accueillant les journées européennes du patrimoine les 21 et 22 septembre 2019, ainsi que sur l'ensemble des infrastructures et sites destinés à accueillir les participants au sommet du G7 à Biarritz du 25 au 27 aout 2019.

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

2.3. Sécurité des établissements scolaires, de l'enseignement supérieur et des structures d'accueil collectif de mineurs (ACM)

2.3.1 Contexte général

La fin de l'année scolaire 2018-2019 et la promulgation des résultats des examens et concours, les déplacements et voyages scolaires traditionnellement nombreux à cette période, les activités estivales des accueils collectifs de mineurs et des universités ainsi que la rentrée scolaire 2019-2020 constituent autant de vulnérabilités qui doivent relever le niveau de vigilance et nécessitent le développement d'une culture commune de gestion de crise dont l'un des objectifs est d'accroître l'interopérabilité avec les services préfectoraux, les FSI et les mairies.

Les établissements privés hors contrat, les établissements de l'enseignement supérieur, les ACM à caractère éducatif, ainsi que les établissements sous tutelle des MEF, devront être acteurs des dispositions préconisées.

2.3.2 Objectifs de sécurité recherchés sur la période

➢ *Reconduction des principales mesures VIGIPIRATE*

Les manifestations de fin d'année scolaire 2018-2019, les activités estivales des universités et la rentrée scolaire 2019-2020 feront l'objet de mesures de sécurité adaptées : assurer la surveillance, le contrôle et filtrage des flux, éviter les attroupements aux abords des établissements, afficher le logo d'alerte VIGIPIRATE en vigueur et les consignes de sécurité.

La sécurité des déplacements scolaires et ceux hors période scolaire prévus par les ACM doit être assurée : éviter les attroupements et les stationnements inutiles sur la voie publique ou aux abords des gares, pour les voyages à l'étranger, les consignes diffusées par le ministère de l'Europe et des affaires étrangères (MEAE) doivent être respectées par les structures organisatrices (Cf. § 2.5).

La protection et l'accès au stockage des matériels et des produits sensibles ou toxiques doivent être assurés : garantir une surveillance accrue et une mise à jour régulière des inventaires afin de détecter rapidement les vols et disparitions.

➢ *Sécurisation des bâtiments*

L'élaboration ou la réalisation des mises à jour nécessaires des diagnostics de sûreté et des Plans particuliers de mise en sûreté (PPMS) « attentat-intrusion » et la réalisation des exercices annuels associés, sont à poursuivre.

Pour les ACM, il convient de renforcer la surveillance des accès aux centres de loisirs.

➢ *Collaboration entre les gouvernances académiques, universitaires, les services départementaux des préfectures et les FSI*

Le partage d'informations entre les différents acteurs doit être favorisé : coordonnées, PPMS, plans bâtimentaires.

2.4. Sécurisation des sites touristiques

2.4.1 Contexte général

La période estivale et la rentrée marquent deux pics de l'activité touristique et culturelle dans notre pays.

Outre la reprise de l'enseignement, le mois de septembre verra aussi l'organisation de la 36ème édition des journées européennes du patrimoine les 21 et 22 septembre 2019[3].

2.4.2 Objectifs de sécurité recherchés sur la période

Il est rappelé que la sécurisation des files d'attentes et des rassemblements sur la voie publique peut revêtir une grande variété de formes adaptées aux différents environnements et aux contraintes esthétiques et architecturales.

Pour parfaire la sécurité des lieux de rassemblement, le ministère de l'intérieur vient de publier et de diffuser un guide de bonnes pratiques. Outil pédagogique d'aide à la décision, destiné aux organisateurs d'événements de voie publique, ce manuel s'appuie sur des infographies synthétiques leur permettant de disposer rapidement des informations clés.

Diffusé au mois d'octobre 2018 ce guide 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

L'attention portée aux entrées et aux sorties 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 FSI.

Concernant les journées européennes du patrimoine, les établissements y participant doivent prendre connaissance des recommandations en matière de sûreté. Ils sont en outre invités à prendre contact localement avec les FSI afin de les informer des conditions d'ouverture exceptionnelles pendant ce weekend.

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'exercice dans la perspective de valider les procédures internes de confinement ou d'évacuation en cas d'attaque directe ou à proximité.

[3] Une fiche pratique « *Journées européennes du patrimoine : comment sécuriser son établissement face à la menace terroriste ?* » figure en annexe 4 de cette posture.

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

2.5.1 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 de l'Etat français 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.

2.5.2 Objectifs de sécurité recherchés sur la période

Les actions et mesures de protection des ressortissants français, résidents ou de passage à l'étranger, relèvent de l'information et de la sensibilisation :

Edition des « *Conseils aux voyageurs* », régulièrement mise à jour[4].

Suivi personnalisé des 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).

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.

2.6. Sécurité du numérique

2.6.1 Contexte général

Les menaces visant les administrations et les entreprises privées restent élevées et variées. Les événements majeurs de la période feront l'objet d'une attention particulière face aux principaux modes d'action malveillants actuellement observés (attaques par rançongiciels, attaques indirectes et compromission d'équipements réseaux).

2.6.2 Objectifs de sécurité recherchés sur la période

Les opérateurs et les administrations mettent en œuvre une politique de mot de passe suffisamment robuste et n'autorisent pas les utilisateurs du système d'information (SI) à utiliser des mots de passe par défaut ou facilement devinables.

Enfin, compte tenu de la menace persistante liée aux programmes malveillants portant atteinte à l'intégrité et se propageant sur les SI (rançongiciels[5]), 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.

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 programme automatisé en s'assurant que les éléments sauvegardés ne soient pas accessibles par un quelconque réseau, y compris avec des comptes d'administration.

---

[4] Une fiche pratique « *Comment préparer ses déplacements et voyages à l'étranger* » figure en annexe 5 de cette posture.

[5] Une fiche pratique « *Sécurité du numérique. Rançongiciel : vos données prises en otage* » figure en annexe 6 de cette posture.

2.7. Consignes particulières de vigilance, prévention et protection

2.7.1 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 des mesures de sécurité à appliquer par leurs autorités de tutelle.

2.7.2 Sensibilisation à la menace des attaques par véhicule-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 ;
- le guide du ministère de l'intérieur évoqué au § 2.4.

2.8. Sensibilisation du grand public

2.8.1 Efforts de communication

Les opérateurs publics et privés mettent en place les logogrammes du niveau d'alerte VIGIPIRATE en vigueur : **« *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 opérateurs sont invités à relayer le plus largement possible les principales mesures de cette posture VIGIPIRATE ainsi que les outils de sensibilisation à la menace terroriste téléchargeables sur les deux sites cités *supra*.

2.8.2 Sensibilisation des professionnels et du grand public aux bonnes pratiques

Dans un souci de pédagogie et de large diffusion des bonnes pratiques face à la menace terroriste, cette posture comporte, en annexe, des fiches de sensibilisation à destination, tant du grand public que des professionnels. Ces fiches sont accessibles sur le site Internet du SGDSN ainsi que 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 régulièrement renouvelée et renforcée. Cette communication peut se faire par le biais de deux documents téléchargeables sur le site du Gouvernement (http://www.gouvernement.fr/reagir-attaque-terroriste) :

- l'affiche « *Réagir en cas d'attaque terroriste* ». Elle 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) ;
- l'affichette « *Les gestes d'urgence si quelqu'un a été blessé autour de vous* ». Elle délivre des messages simples et concis pour expliquer comment réaliser les premiers gestes d'urgence en attendant l'arrivée des secours.

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.

Enfin, le SGDSN réalise actuellement une plateforme de sensibilisation à destination des citoyens, des responsables d'établissement recevant du public et des élus locaux. Cette plateforme vise à sensibiliser l'ensemble des citoyens aux bons comportements à adopter afin de prévenir ou de réagir à un acte terroriste. Elle sera accessible sur Internet dans le courant du deuxième semestre 2019. Une communication spécifique sera réalisée lors du lancement de cette plateforme.

Il vous est demandé de diffuser cette posture VIGIPIRATE « *Eté - Rentrée 2019* » à l'ensemble de vos services ou adhérents, **sans que cela ne se traduise par une publication en accès libre sur vos sites internet.**

Le Haut fonctionnaire de défense et de sécurité adjoint

Christian DUFOUR

3. ANNEXES

Annexe 1 : Tableau des principaux événements organisés sur le territoire national.

Diffusion sans restriction.

Annexe 2 : Infographie des attentats jihadistes réalisés, échoués, déjoués en France et dans les pays limitrophes en 2018.

Diffusion sans restriction.

Annexe 3 : Cartographie des attentats jihadistes réalisés, échoués, déjoués en France depuis 2015.

Diffusion sans restriction.

Annexe 4 : Fiche pratique « Journées européennes du patrimoine : comment sécuriser son établissement face à la menace terroriste ? ».

Diffusion sans restriction.

Annexe 5 : Fiche pratique « Comment préparer ses déplacements et voyages à l'étranger ? ».

Diffusion sans restriction.

Annexe 6 : Fiche pratique « Sécurité du numérique. Rançongiciel : vos données prises en otage ».

Diffusion sans restriction.

Annexe 7 : Liste des différentes fiches pratiques VIGIPIRATE en vigueur

Diffusion sans restriction.

Annexe 1 : Tableau des principaux événements organisés sur le territoire national

mai 2019

Date	Lieu	Evénement	Type d'événements	Affluence estimée
27 avril au 8 mai	Paris – Porte de Versailles (75)	Foire de Paris	Economique	500.000
6 mai	Ensemble du Territoire national	Début du Ramadan	Religieux	/
8 mai	Ensemble du Territoire national	Fête de la Victoire (férié)	Commémoratif	/
13 au 16 mai	Bordeaux - Parc des expositions (33)	Vinexpo	Economique	30.000 par jour (chiffre de 2018)
16 au 18 mai	Paris – Porte de Versailles (75)	Salon Viva Technology	Economique	60.000
26 mai	Ensemble du Territoire national	Elections européennes	Politique	/
30 mai	Ensemble du Territoire national	Ascension (fête chrétienne et jour férié)	Religieux	/

juin 2019

Date	Lieu	Evénement	Type d'événements	Affluence estimée
Juin à août	Saint-Germain-en-Laye (78)	Fête des Loges (fête foraine)	Economique	3 millions (chiffre 2018)
1er juin	Ensemble du Territoire national	Laylat al-Qadr (fête musulmane)	Religieux	/
4 juin	Paris - Champs-Elysées (75)	Paris Drone Festival	Economique	200 000 (chiffre 2018)
4 au 10 juin	Normandie	Commémorations du 75e anniversaire du Débarquement	Commémoratif	/
4 au 10 juin	Paris (75) Champ-de-Mars	75e anniversaire du débarquement	Commémoratif	
5 juin	Ensemble du Territoire national	Aïd el-fitr (fête musulmane célébrant la fin du jeune du Ramadan)	Religieux	/
7 juin	Paris (75)	« G7 social » pour l'Emploi	Diplomatique	
8 au 10 juin	Ensemble du Territoire national	Chavouot (fête juive)	Religieux	/
9 juin	Ensemble du Territoire national	Pentecôte (fête chrétienne et jour férié)	Religieux	/
10 juin	Ensemble du Territoire national	Lundi de Pentecôte (jour férié)	Religieux	/
10 au 15 juin	Annecy (74)	Festival international du film d'animation	Economique	30.000
13 juin	Ensemble du Territoire national	3e anniversaire de l'attaque sur un couple de policiers de Magnanville	Commémoratif	/

Date	Lieu	Evénement	Type d'événements	Affluence estimée
17 au 23 juin	Paris – Le Bourget (93)	Salon International de l'Aéronautique et de l'Espace	Economique	375.000
17 au 24 juin	Ensemble du Territoire	Baccalauréat	/	
24 juin	Marseille (13)	« Sommet des deux rives » (sommet de la Méditerranée)	Diplomatique	/
26 juin	Ensemble du Territoire national	4e anniversaire de l'attaque de Saint Quentin Fallavier	Commémoratif	/
26 juin au 6 août	Ensemble du Territoire national	Soldes d'été	Economique	/

juillet 2019

Date	Lieu	Evénement	Type d'événements	Affluence estimée
A compter du 5 juillet	Ensemble du Territoire national	Résultats du bac : attroupements devant les lycées	/	/
7 juillet	Ensemble du Territoire national	Début vacances été (afflux gares aéroports)	Congés	/
14 juillet	Ensemble du Territoire national	Fête nationale (férié)	/	/
14 juillet	Paris – Champs de Mars (75)	Feu d'artifice	Festivités	500.000 (estimation)
22 et 23 juillet	Ensemble du Territoire national	Tisha Beav (fête juive)	Religieux	/
26 juillet	Ensemble du Territoire national	3e anniversaire des attentats de Saint Etienne du Rouvray	Commémoratif	/

août 2019

Date	Lieu	Evénement	Type d'événements	Affluence estimée
11 août	Ensemble du Territoire national	Jeûne du 9 Av (fête juive)	Religieux	/
11 août	Ensemble du Territoire national	Aïd el-Kébir (fête musulmane)	Religieux	/
13 au 16 août	Provence	Commémorations du 75e anniversaire du Débarquement	Commémoratif	/
Date	**Lieu**	**Evénement**	**Type d'événements**	**Affluence estimée**
15 août	Ensemble du territoire national	Assomption (fête chrétienne et jour férié)	Religieux	25.000 pèlerins à Lourdes
19 au 25 août	Paris	75e anniversaire de la Libération de Paris	Commémoratif	/
21 août	Ensemble du Territoire national	4e anniversaire de l'attaque du Thalys	Commémoratif	/
24 au 26 août	Biarritz (64)	G7	Diplomatique	/
31 août au 1er septembre	Lille (59)	Grande braderie	Economique	2,5 millions

septembre 2019

Date	Lieu	Evénement	Type d'événements	Affluence estimée
1er septembre	Ensemble du Territoire national	Raas Assana – Nouvel an musulman	Religieux	/
2 septembre	Ensemble du Territoire national	Rentrée scolaire	/	/
10 septembre	Ensemble du Territoire national	Achoura (plus importante fête chiite ; jour de jeûne pour les sunnites)	Religieux	/
12 au 17 septembre	Paris – Grand Palais (75)	Biennale de Paris	Economique/ Culturel	33.000
14 septembre	Ensemble du Territoire national	Exaltation de la Croix (grande fête orthodoxe)	Religieux	/
29 septembre au 1er octobre	Ensemble du Territoire national	Roch ha-Chanah (Nouvel an juif)	Religieux	/

octobre 2019

Date	Lieu	Evénement	Type d'événements	Affluence estimée
9 octobre	Ensemble du Territoire national	Yom Kippour (Grand Pardon)	Religieux	/
17 au 20 octobre	Paris (75)	FIAC (Foire internationale d'art contemporain)	Economique/ Culturel	70.000
20 octobre	Ensemble du Territoire national	Vacances scolaires de la Toussaint	Congés	/

Légende

	Commémorations
	Congés
	Fêtes religieuses

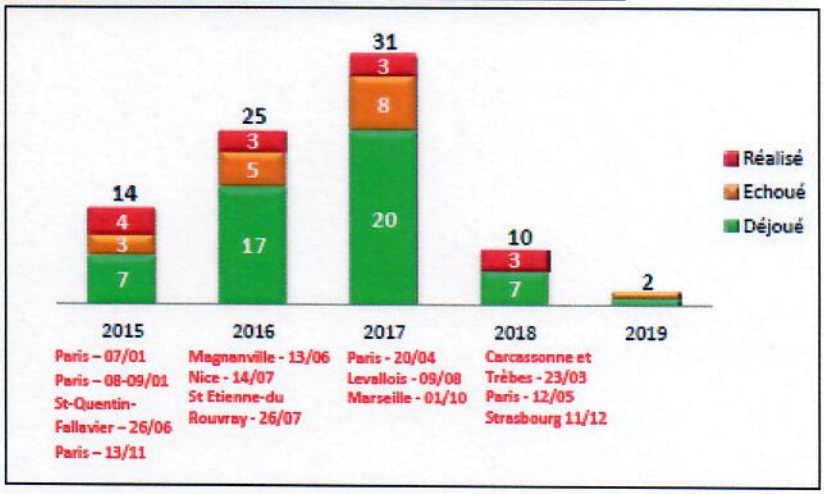
Annexe 2 : Infographie sur les attentats jihadistes réalisés, déjoués, échoués en France depuis 2015.

SGDSN — Bva Bureau de veille et d'alerte

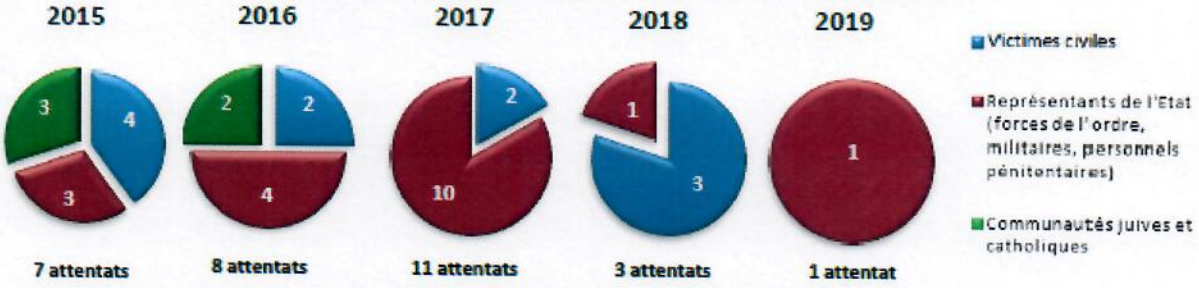
HISTORIQUE DES ATTENTATS JIHADISTES EN FRANCE DE 2015 A 2019

RECAPITULATIF DES ATTENTATS REALISES, ECHOUES OU DEJOUES

Sur le territoire national, la menace se maintient à un niveau élevé malgré une baisse de la fréquence des attaques et projets d'attaques en 2018 et au premier trimestre 2019. Les trois dernières années ont chacune été marquées par trois attentats réalisées



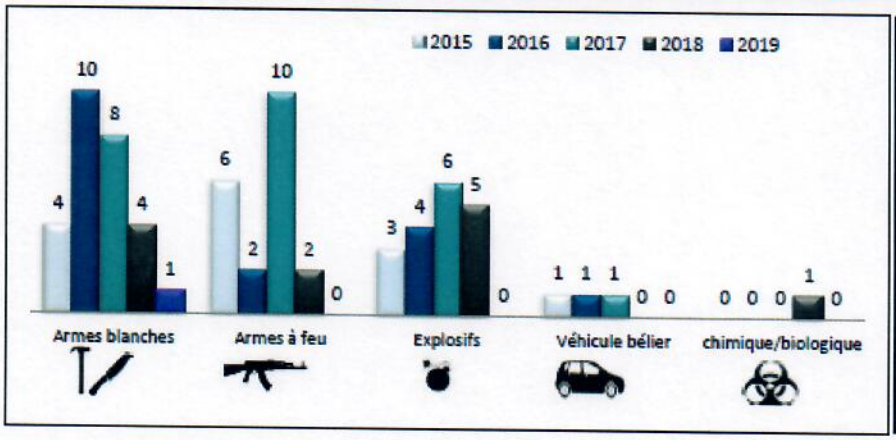
TYPES DE CIBLES VISEES LORS DES ATTENTATS REALISES OU ECHOUES**



** *plusieurs cibles ont parfois été visées lors d'un même attentat.*

Les représentants en uniforme de l'autorité publique (forces de l'ordre, militaires, personnels pénitentiaires) demeurent les premières cibles visées par les assaillants lors d'attentats, suivies de la population civile : deux cibles relativement facilement atteignables. Les cibles du terrorisme jihadiste visées pour leur appartenance religieuse sont en baisse sur la période mais le risque demeure latent.

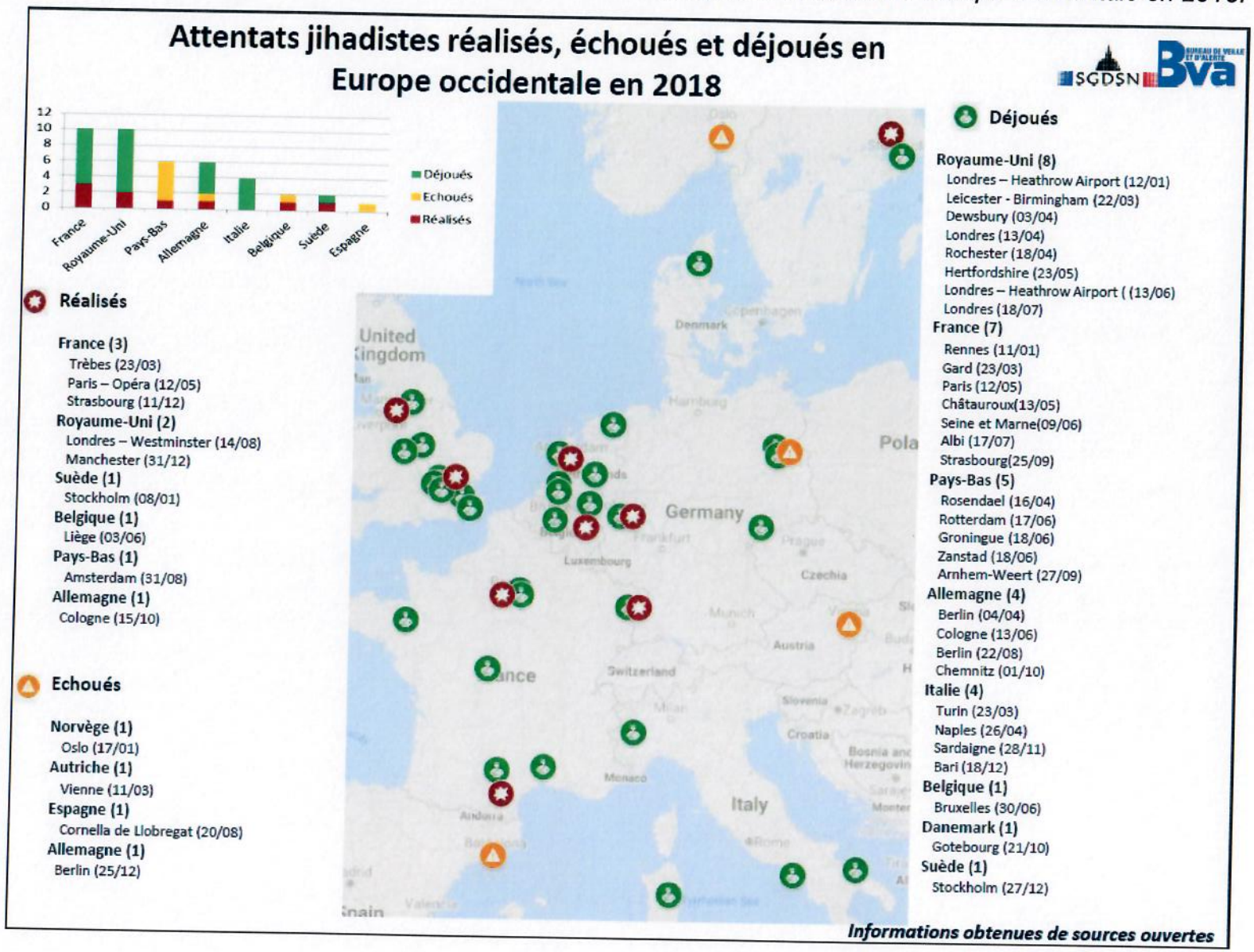
MODES OPERATOIRES UTILISES LORS DES ATTENTATS ABOUTIS, ECHOUES, DEJOUES



De façon générale sur la période les modes opératoires sommaires (utilisation d'armes par destination) demeurent les plus fréquemment utilisés (armes blanches, armes à feu, véhicule-bélier). Toutefois certains modes opératoires plus sophistiqués tels que des engins explosifs improvisés voire l'utilisation de substances chimiques ou d'agents toxiques ne doivent pas être négligés.

Informations obtenues de sources ouvertes

Annexe 3 : Cartographie des attentats jihadistes réalisés, déjoués, échoués en Europe occidentale en 2018.



Annexe 4 : Fiche « Journées européennes du patrimoine : comment sécuriser son établissement face à la menace terroriste ? »

JOURNÉES EUROPÉENNES DU PATRIMOINE

Comment sécuriser son établissement face à la menace terroriste

Fiche actualisée en date du 7 mai 2019

Fiche pratique à destination des particuliers propriétaires de lieux patrimoniaux, des services de l'Etat et des responsables d'établissements ou de sites accueillant du public à l'occasion des Journées européennes du patrimoine.

Tout responsable d'établissement ou de site accueillant du public est encouragé à décliner **le plan VIGIPIRATE** dans son propre plan de sûreté. L'Etat incite particulièrement les établissements accueillant du public à **établir des procédures de réaction en cas d'attaque terroriste et à sensibiliser leurs employés, bénévoles et volontaires.**

À cette fin, les autorités ont rédigé, en liaison avec les acteurs concernés, un **ensemble de guides de bonnes pratiques** à destination des responsables d'établissements, culturels et patrimoniaux, disponibles sur les sites du SGDSN (www.sgdsn.gouv.fr/plan-vigipirate), du ministère de la culture[1] et du Gouvernement[2]. Cette fiche pratique complète les mesures de sûreté définies à l'occasion des Journées européennes du patrimoine des 21 et 22 septembre 2019.

1 Se préparer à faire face à une crise

Analyser les vulnérabilités de votre établissement pour identifier vos axes d'effort.

- En quoi votre établissement pourrait être une cible (site représentant les institutions du pays, site symbolique du mode de vie occidental ou des valeurs de la République française, lieu de culte, etc.) ?
- Qu'est-ce qui pourrait être ciblé dans votre établissement (personnel, infrastructures, informations, matériels spécifiques, etc.) ?
- Identifier les vulnérabilités physiques de l'établissement (nombre d'accès, portes ne fermant pas à clef, point de livraison, etc.).
- Prendre en considération la menace interne à votre établissement (signalement d'un cas de radicalisation par exemple).

Sensibiliser l'ensemble des collaborateurs aux consignes de sûreté et de sécurité, en s'appuyant sur les fiches de recommandations et guides disponibles sur le site du *Secrétariat général de la défense et de la sécurité nationale* :

http://www.sgdsn.gouv.fr/plan-vigipirate/

Disposer d'un annuaire à jour (police, secours, etc.) et de deux numéros de téléphone (le responsable de l'établissement et la personne désignée pour centraliser l'information) à contacter en cas de crise et transmis aux forces de sécurité intérieure compétentes ainsi qu'aux éventuels partenaires qui pourraient être impliqués (établissements proches, sous-traitants, etc.).

Tester les moyens d'alerte (vers la police nationale, la gendarmerie nationale, les services de secours, etc.) et le dispositif de crise.

2 Gérer la sûreté pendant l'événement

2.1 - Sûreté externe

Développer les relations avec les partenaires extérieurs. Il est important d'identifier et de connaître les différents acteurs qui pourraient être amenés à jouer un rôle dans le dispositif de gestion de crise :

- le préfet et les services de l'Etat ;
- le maire et les services municipaux ;
- les forces de police et de gendarmerie ;
- les services de secours les plus proches.

1 - http://www.culture.gouv.fr/Espace-documentation/Rapports/GERER-LA-SURETE-ET-LA-SECURITE-DES-EVENEMENTS-ET-SITES-CULTURELS
2 - http://www.gouvernement.fr/reagir-attaque-terroriste

Fiche actualisée en date du 7 mai 2019

Les actions ci-dessous sont à privilégier :

- anticiper les files d'attente et éviter au maximum les attroupements à l'extérieur de l'établissement ;
- préférer des espaces protégés de la circulation des véhicules ;
- insister sur les conditions de stationnement et de circulation aux abords des installations ;
- rendre visible le logo représentant le niveau d'alerte VIGIPIRATE ;
- communiquer sur les conditions d'accès au site notamment pour les visiteurs avec sacs et bagages.

2.2 - Sûreté interne

- Prévoir des équipements adaptés aux ressources du site et à sa configuration.
- Distinguer de manière formelle les espaces ouverts au public des espaces qui ne le sont pas avec, de préférence, une fermeture mécanique.
- Mettre en place un système d'alarme en interne (tel qu'un sifflet, un haut-parleur, etc.) et un moyen d'alerte vers les autorités. Et si les lieux s'y prêtent, envisager un espace de confinement.

2.3 - Vigilance et contrôle des accès

- Renforcer la vigilance et le contrôle des accès, s'appuyer sur la vidéoprotection si elle existe.
- Restreindre le nombre d'accès à l'établissement en fonction des capacités de surveillance. Cette mesure ne devra pas entraîner une diminution du nombre de sorties de secours.
- **Mettre en place un contrôle des accès** et aménager un espace pour effectuer ce contrôle. Les mesures de surveillance statique ou d'inspection visuelle aux entrées peuvent être confiées **soit à la police municipale** (article L. 511-1 du Code de la sécurité intérieure, sur décision du maire, complété par l'article 21 de la loi du 28 février 2017 relative à la sécurité publique), soit à des **agents de sécurité privée** (article L. 613-2 du Code de la sécurité intérieure) ;
- Mettre en place une surveillance, même aléatoire, de la file d'attente.

Comment réagir ? :

Dès que vous êtes en sécurité, appelez le 17 ou le 112

Si l'attaque est extérieure au site dans lequel vous vous trouvez, il est recommandé de rester à l'abri.

Si l'attaque a lieu à l'intérieur du site où vous vous trouvez, échappez-vous, ou si cela est impossible, cachez-vous.

Dans tous les cas, donnez l'alerte. Une fois en sécurité, prévenez les forces de sécurité (17, 112 ou 114).

Prévenez, si possible, les sites aux alentours.

3 Etre vigilant jusqu'à la fin de l'événement

Maintenir le niveau de vigilance tout au long de l'événement et lors du moment sensible de sa dispersion. Il conviendra de procéder à une **ronde de fermeture** avec un contrôle de tous les espaces ouverts au public.

Il est important **de procéder à un retour d'expérience simple** de l'événement qui s'est déroulé pour en identifier les points forts ainsi que les axes d'amélioration.

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 : Pôle graphique, fabrication, image – DSAF/DPGS – Mai 2019.

Annexe 5 : Fiche « Comment préparer ses déplacements et voyages à l'étranger ? »

COMMENT PRÉPARER SES DÉPLACEMENTS ET VOYAGES À L'ÉTRANGER ?

VIGIPIRATE

Fiche actualisée en date du 7 mai 2019

Il est recommandé aux personnes se rendant à l'étranger de prendre un certain nombre de précautions afin de garantir leur sécurité personnelle. Cette fiche précise comment préparer son voyage et comment réagir en cas de survenue d'une attaque terroriste alors que l'on se trouve dans un pays étranger.

1 Avant le départ

S'informer

Sur la sécurité dans le pays

- La rubrique « Conseils aux voyageurs » du site Internet du ministère de l'Europe et des affaires étrangères vous informe sur les risques propres à chaque pays et les précautions à prendre.
- Les fiches pays vous renseignent sur les problèmes de sécurité, la fiabilité des moyens de transport, les risques sanitaires et les conditions d'hygiène locale, les us et coutumes et la législation locale.
- Il est important de choisir un circuit touristique ou un lieu de villégiature qui offre le maximum de sécurité. Les cartes de la rubrique « Conseils aux voyageurs » vous indiquent, pour chaque pays, le degré de sécurité de ses différentes régions.
- Les zones rouges sont formellement déconseillées, car elles peuvent représenter un risque élevé pour votre vie et votre sécurité.
- Les zones orange sont déconseillées sauf raisons impératives (professionnelle ou familiale).

Planifier

- Il est nécessaire de souscrire aux assurances adaptées (notamment rapatriement / hospitalisation) lorsque vous vous rendez à l'étranger.
- Pensez à enregistrer les numéros d'urgence locaux, de votre assurance et du consulat. Il existe des services consulaires dans la plupart des pays.

Inscrivez-vous sur le service en ligne gratuit « Ariane »

Pourquoi s'inscrire ?

Créé par le ministère de l'Europe et des affaires étrangères, le site Ariane permet à tout ressortissant français, lors d'un voyage ou d'une mission ponctuelle à l'étranger, de se signaler afin de bénéficier, par mail, SMS ou téléphone, d'informations et de consignes de sécurité en temps réel dans le pays de villégiature. Ariane permet également aux autorités françaises, en cas de crise, de connaître votre présence dans un pays.

http://diplomatie.gouv.fr/ariane

L'inscription sur le site Ariane, conçue en concertation avec la CNIL, offre toutes les garanties de sécurité et de confidentialité des données personnelles. Elle ne se substitue pas à l'inscription au registre des Français établis hors de France dès lors que le temps de séjour est supérieur à 6 mois.

Pour plus d'informations vous pouvez vous rendre sur le site du ministère de l'Europe et des affaires étrangères : *https://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/*

COMMENT PRÉPARER SES DÉPLACEMENTS ET VOYAGES À L'ÉTRANGER ?

Fiche actualisée en date du 7 mai 2019

2 Les principaux réflexes à adopter en cas d'attaque terroriste

Si jamais vous êtes confronté à une attaque terroriste à l'étranger, vous devez, comme vous le feriez en France, adapter vos réactions aux circonstances.

Si l'attaque est extérieure au site dans lequel vous vous trouvez, il est recommandé de rester à l'abri.

Si l'attaque a lieu à l'intérieur du site où vous vous trouvez, respectez les consignes de sécurité présentées ci-dessous.

S'échapper

Condition 1 : être certain que vous avez identifié la localisation exacte du danger.

Condition 2 : être certain de pouvoir vous échapper sans risque.

Dans tous les cas : Ne déclenchez pas l'alarme incendie.

- Laissez toutes vos affaires sur place ;
- Ne vous exposez pas (courbez-vous, penchez-vous) ;
- Prenez la sortie la moins exposée et la plus proche ;
- Utilisez un itinéraire connu ;
- Aidez si possible les autres personnes à s'échapper ;
- Prévenez / alertez les autres personnes autour de vous ;
- Dissuadez toute personne de pénétrer dans la zone de danger.

Se cacher

- Dans la mesure où vous ne pouvez pas vous échapper, enfermez-vous, barricadez-vous, cachez-vous dans un endroit hors de la portée des agresseurs ;
- Condamnez la porte si celle-ci n'a pas de serrure en bloquant la poignée avec des moyens de fortune (meuble, etc.) ;
- Éteignez les lumières ;
- Éloignez-vous des murs, portes et fenêtres ;
- Allongez-vous au sol derrière plusieurs obstacles solides (des projectiles tirés au travers des cloisons peuvent atteindre l'intérieur de la pièce dans laquelle vous vous trouvez) ;
- Faites respecter le silence absolu (portables en mode silence, sans vibreur) et décrochez les téléphones fixes ;
- Restez proche des personnes manifestant un stress et rassurez-les, attendez l'intervention des forces de sécurité.

Alerter

- Une fois en sécurité : prévenez les forces de sécurité **(numéro d'appel d'urgence européen : 112 ; ou numéro spécifique du pays où vous vous trouvez)** ;
- Où ? Donnez votre position mais également celle de vos agresseurs ;
- Quoi ? Nature de l'attaque, estimation du nombre d'assaillants, description (sexe, vêtements, physionomie, signes distinctifs...), attitude (comment se comportent-ils, regardent-ils la télévision, ont-ils des moyens de communication...).
- Suivez les consignes des autorités locales : elles sont responsables de la sécurité des personnes se trouvant sur leur territoire, quelle que soit leur nationalité.

3 Que faire après une attaque

116 006
Numéro d'aide aux victimes

- **Informez vos proches de votre situation, quand cela est possible, par tous les moyens à disposition (SMS, appels, réseaux sociaux) ;**
- **Contactez le 116 006, plateforme téléphonique nationale d'écoute et d'information des victimes ;**
- **Hors France métropolitaine, composez le +33 (0)1 80 52 33 76 (numéro non surtaxé) ;**
- Des écoutants professionnels vous offrent une écoute privilégiée, une identification des besoins et des premiers conseils, 7 jours sur 7 ;
- Vous pourrez être mis en relation avec une association d'aide aux victimes et/ou tout service ou administration susceptible de répondre à vos demandes.

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 : Pôle graphique, fabrication, image – DSAF/DPSS – Avril 2019.

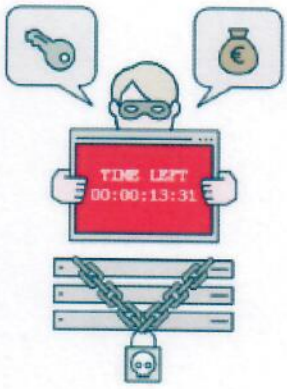
Annexe 6 : Fiche « Sécurité du numérique. Rançongiciel : vos données prises en otage »

VIGIPIRATE

SÉCURITÉ DU NUMÉRIQUE
RANÇONGICIEL : VOS DONNÉES PRISES EN OTAGE

Cible : tous publics

- Un rançongiciel (*ransomware* en anglais) est un programme malveillant dont le but est de chiffrer partiellement ou entièrement les données d'un système, bloquant ainsi leur accès.
- La machine peut être infectée après l'ouverture d'une pièce-jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en navigant sur des sites compromis, ou encore suite à une intrusion dans le système.
- Le principal but recherché est d'extorquer de l'argent à la victime en échange de la promesse (pas toujours tenue) de retrouver l'accès aux données corrompues. Si l'intention de ce type d'attaque est cybercriminelle, le mode opératoire de ces attaques peut être lourd de conséquences pour les victimes qui peuvent par exemple voir leur activité paralysée.
- Particulièrement répandues, ces attaques sont de plus en plus sophistiquées et peuvent toucher l'ensemble des acteurs de la société, qu'il s'agisse de citoyens ou d'organisations publiques ou privées.



1 Comment réagir ?

1- N'éteignez pas la machine concernée

L'interruption du processus de chiffrement empêche toute tentative ultérieure de récupération des données.
Mettez la machine en veille prolongée si possible.

2- Déconnectez immédiatement du réseau les machines concernées

L'objectif est de limiter la propagation de l'attaque en bloquant la poursuite du chiffrement des documents sur le réseau.
Ne connectez pas non plus d'appareil supplémentaire sur le réseau.

3- Contactez immédiatement votre service informatique ou un expert

Vous êtes un ministère, un opérateur d'importance vitale (OIV), un opérateur de service essentiel (OSE) ou un fournisseur de service numérique (FSN) ?

→ Prévenez l'ANSSI :
www.ssi.gouv.fr/en-cas-dincident/

Vous êtes une collectivité territoriale, une entreprise privée (non OIV, non OSE), une association ?

→ Contactez si besoin cybermalveillance :
www.cybermalveillance.gouv.fr

4- Ne payez pas la rançon réclamée

Le paiement ne garantit pas le déchiffrement des données et compromettra le moyen de paiement utilisé.

SÉCURITÉ DU NUMÉRIQUE
RANÇONGICIEL : VOS DONNÉES PRISES EN OTAGE

5- Portez plainte auprès des services compétents

Pensez à réunir toutes les traces et indices qui pourraient servir comme éléments de preuve (ex : copies physiques de disques durs des postes compromis).

6- Identifiez la source de l'infection

Prenez les mesures nécessaire pour que la source de l'infection ne puisse pas être utilisée à nouveau (par l'application d'un correctif de sécurité par exemple).

2 Comment se protéger ?

Effectuez des sauvegardes régulières de vos données critiques

Ces sauvegardes vous permettent de limiter le préjudice de l'incident et de reprendre vos activités rapidement. Les supports de ces sauvegardent doivent être déconnectées physiquement du réseau afin d'éviter toute compromission en cas d'incident. Faites également des tests de restauration de sauvegarde réguliers afin de vérifier votre capacité à restaurer vos données en cas d'incident.

Mettez à jour régulièrement vos logiciels

Les rançongiciels utilisent les vulnérabilités des programmes pour se propager, appliquez-donc de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur vos systèmes.

Privilégiez un compte utilisateur pour vos usages courants

N'utilisez pas un compte avec des droits « administrateurs » pour consulter vos messages ou naviguer sur Internet.

Méfiez-vous des messages douteux

Ne faites pas confiance à l'expéditeur de courriers électroniques dont l'origine ou la forme vous semble douteuse et méfiez-vous des pièces-jointes et des liens suspects. Il convient en effet de ne pas cliquer sans vérification sur les liens ni d'ouvrir les pièces jointes présentes ; une attention toute particulière devant être apportée aux messages de provenance inconnue, d'apparence inhabituelle ou frauduleuse.

3 En savoir plus

Les bonnes pratiques de l'informatique :
www.ssi.gouv.fr/precautions-elementaires/

Guide d'hygiène informatique (à l'attention des DSI)
https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

En cas d'incident : https://www.ssi.gouv.fr/en-cas-dincident/

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 : Pôle graphique, édition, image – DSAF/DPGS – Avril 2018.

Annexe 7 : Liste des différentes fiches pratiques VIGIPIRATE en vigueur diffusées sur le site Internet du SGDSN

Intitulé de la fiche	Date de diffusion	Cible(s) visée(s)
Signalement de situations suspectes : recommandations à l'usage du grand public	Juin 2017	Grand public
Organiser un confinement face à une menace terroriste	Octobre 2017	Responsables sécurité / sûreté des établissements recevant du public
Produits chimiques : signalement de tout vol ou utilisation suspecte	Octobre 2017	Grand public Professionnels commercialisant des produits chimiques
Sécurité du numérique : l'hameçonnage (ou *phishing*)	Octobre 2017	Personnels des organismes publics et privés
Recommandations pour la sécurisation des lieux de rassemblement ouverts au public	Février 2018	Organisateurs de rassemblements ouverts au public
Prévention et signalement de cas de radicalisation djihadiste	Février 2018	Grand public
Sécurité du numérique : Sensibilisation des dirigeants	Février 2018	Dirigeants d'entreprises privées ou de collectivités territoriales
Se protéger contre les attaques au véhicule-bélier	Juin 2018	Organisateurs d'événements de voie publique
Attaques au véhicule-béliers : recommandations à l'attention des gestionnaires de parcs et loueurs de véhicule	Juin 2018	Gestionnaires de parcs et loueurs de véhicule
Drones : règles d'utilisation et mesures de prévention face à un usage malveillant	Juin 2018	Organisateurs de manifestations sur le domaine public
Comment préparer ses déplacements et voyages à l'étranger ?	Mai 2019	Grand public
Journées européennes du patrimoine : comment sécuriser son établissement face à la menace terroriste ?	Mai 2019	Particuliers propriétaires de lieux patrimoniaux Services de l'Etat et responsables de sites accueillant les journées européennes du patrimoine
Sécurité du numérique. Rançongiciel : vos données prises en otage	Mai 2019	Grand public