La posture VIGIPIRATE « *Printemps 2018* » s'applique, sauf événement particulier, du 1ier mars 2018 au 13 juin 2018. Cette période est marquée par l'organisation de grands événements ou manifestations à caractère culturel, social, sportif ou religieux. Ces événements requièrent une mobilisation accrue des acteurs de la sécurité, qu'ils soient publics ou privés.

1. Principaux événements sur le territoire national

Les tableaux ci-après dressent la liste des principaux événements organisés sur le territoire national au cours des quatre prochains mois. Cette liste est non exhaustive.
Les vacances et les jours fériés ont été surlignés pour plus de lisibilité.

MARS 2018	Lieu	Evénement	Affluence estimée
24 février au 4 mars	Paris (porte de Versailles) - Parc des expositions	Salon international de l'Agriculture	620 000 (chiffre 2017)
1er mars	Paris - Bataclan	Concert du groupe de rock australien *King Gizzard & the lizard*	Capacité maximale 1 500
4 mars	Paris	Semi-marathon de Paris	38 000 (chiffre 2017)
6 mars	Paris - Parc des Princes	Ligue des champions, 8e de finale : PSG – Real Madrid	Capacité maximale 48 500
8 et 9 mars	Paris - Bataclan	Concert du groupe de *heavy metal* américain *Black Label society*	Capacité maximale 1 500
10 mars	Paris - Stade de France	Rugby : Tournoi des six nations France -Angleterre	78 000 (chiffre 2017)
10 au 12 mars	Paris (porte de Versailles) - Parc des expositions	Salon du golf	30 000 (chiffre 2017)
13 mars	Paris - AccorHotels Arena	Concert du chanteur anglais Harry Styles	Capacité maximale 20 300
14 mars	Paris - AccorHotels Arena	Concert du groupe de rock américain *Thirty Seconds to Mars*	Capacité maximale 20 300
15 au 18 mars	Paris (porte de Versailles) - Parc des expositions	Salon du Tourisme	130 000 (chiffre 2017)
16 au 19 mars	Paris (porte de Versailles) - Parc des expositions	38e édition du Salon du Livre	160 000 (chiffre 2017)
17 mars	Paris - Stade de France	Course d'obstacle Spartan Stadium	-
17 au 25 mars	Evénement international	Semaine de la langue française et de la francophonie	-
18 mars	Marseille	Marathon run in Marseille	13 000 (chiffre 2017)
21 mars	Ensemble du Territoire	Date de la mort de Mohammed Merah (2012)	-
22 et 23 mars	Paris - AccorHotels Arena	Concert du groupe *Shaka Ponk*	Capacité maximale 20 300 par jour
23 mars	Paris - Stade de France	Football : France-Colombie	Capacité maximale 81 338
24 mars	Paris - Bataclan	Concert du groupe de métal américain *Machine Head*	Capacité maximale 1 500
24 mars	Bordeaux	4e édition du marathon de Bordeaux	19 720 (chiffre 2017)
24 mars	Lyon - Halle Tony Garnier	Fresque musicale Jésus de Nazareth	Capacité maximale 17 000
25 mars	Ensemble du Territoire	Annonciation (fête chrétienne)	-
25 mars	Paris - AccorHotels Arena	Spectacle *Harlem Globetrotters*	Capacité maximale 20 300
31 mars	Bordeaux	Football : finale de la coupe de la Ligue	Capacité maximale 42 000 places
31 mars	Ensemble du Territoire	Pessah (fête juive commémorant l'exode des Hébreux hors d'Egypte et la fin de leur esclavage)	-

AVRIL 2018	Lieux	Evènements	Affluence estimée
1er avril	Ensemble du Territoire	Pâques (fête chrétienne)	-
2 avril	Ensemble du Territoire	Lundi de Pâques (férié)	-
7 avril au 7 mai	Ensemble du Territoire	Vacances de printemps (toutes zones confondues)	-
8 avril	Paris	Marathon international de Paris	57 000 (chiffre 2017)
11 et 15 avril	Paris - AccorHotels Arena	Spectacle équestre : Finales Longines FEI World Cup	Capacité maximale 20 300 par jour
13 avril	Ensemble du Territoire	Lailat al Miraj (fête musulmane commémorant la montée au ciel de Mahomet et sa rencontre avec Dieu)	-
13 avril	Paris - Bataclan	Concert du groupe de *heavy metal* américain *Machine Head*	Capacité maximale 1 500
15 avril	Paris	5e édition de la *Color Run*	20 000 (chiffre 2016)
20 et 21avril	Paris - AccorHotels Arena	Basketball : finale de la Coupe de France	Capacité maximale 20 300 par jour
21 et 22 avril	Nantes	Marathon et semi-marathon de Nantes	16 000 (chiffre de 2017)
24 au 29 avril	Bourges	Festival musical : Printemps de Bourges	200 000 (chiffre de 2017)
25 au 26 avril	Paris	Sommet international de lutte contre le financement du terrorisme	-
27 avril au 8 mai	Paris (porte de Versailles)	Foire de Paris	500 000
27 avril	Paris - AccorHotels Arena	Spectacle Fun Radio Ibiza Experience	15 000 (chiffre 2017)
28 avril	Paris	Grand prix de formule E	46 000 (chiffre 2017)
30 avril	Paris - AccorHotels Arena	Concert du chanteur américain Sam Smith	Capacité maximale 20 300

MAI 2018	Lieux	Evènements	Affluence estimée
1er mai (mardi)	Ensemble du Territoire	Fête du travail (férié)	-
5 mai	Paris - AccorHotels Arena	Handball : finale de la Coupe de France	Capacité maximale 20 300
6 au 13 mai	Lyon	Festival Musical : Les nuits sonores	140 000 (chiffre 2017)
8 mai (mardi)	Ensemble du Territoire	Fête de la Victoire (férié)	-
8 mai	Paris - Stade de France	Football : finale de la Coupe de France	Capacité maximale 81 338
9 mai	Lyon - Halle Tony Garnier	Concert du chanteur britannique Roger Waters	Capacité maximale 17 000 par jour
9 au 20 mai	Cannes	Le festival de Cannes	130 000
10 mai (jeudi)	Ensemble du Territoire	Ascension (fête chrétienne et jour férié)	-
13 au 16 mai	Bordeaux - Parc des expositions	Vinexpo	30 000 par jour (chiffre de 2017)
16 mai	Lyon - Stade de Lyon	Finale de l'UEFA Europa League	Capacité maximale 59 000
16 mai au 15 juin	Ensemble du Territoire	**Ramadan (fête musulmane. Mois de jeûne marquant son obéissance à Dieu)**	-
16 au 21 mai	Nîmes	Féria	32 000 (chiffre 2017)
19 mai	Paris - AccorHotels Arena	Spectacle de Catch WWE live	Capacité maximale 20 300
19 mai	Ensemble du Territoire	Nuit des musées	-
20 et 21 mai	Ensemble du Territoire	Pentecôte (fête chrétienne et jour férié)	-
21 mai au 10 juin	Paris	Roland Garros	470 000 spectateurs (chiffre 2017)

MAI 2018	Lieux	Evènements	Affluence estimée
24 au 26 mai	Paris (porte de Versailles)	Salon *Viva Technology*	60 000 (chiffre 2017)
26 mai au 10 juin	Normandie	D-DAY *festival Normandy*	170 000 (estimation)
27 mai	La baie du mont St Michel	Marathon du Mont St Michel	5 000 (chiffre 2017)
27 mai	Monaco	Grand Prix de Formule 1	100 000
28 mai	Paris - Stade de France	Football : France-République d'Irlande	Capacité maximale 81 338
29 et 30 mai	Paris - AccorHotels Arena	Concert de la chanteuse américaine Katy Perry	Capacité maximale 20 300 par jour

JUIN 2018	Lieux	Evènements	Affluence estimée
2 juin	Paris - Stade de France	Rugby : Finale du top 14	Capacité maximale 81 338
4 juin	Paris - Champs-Elysées	Paris Drone Festival	180 000 (chiffre 2017)
8 et 9 juin	Paris (92) – U Arena	Concert du chanteur britannique Roger Waters	Capacité maximale 40 000 par jour
11 au 15 juin	Paris - Villepinte	Eurosatory	57 000 (chiffre 2016)
11 au 16 juin	Annecy	Festival international du film d'animation	7 000 chaque soir
13 juin	**Ensemble du territoire**	**Début de la coupe du monde de football en Russie (fans zones à Paris, etc.)**	-
13 juin	Ensemble du Territoire	2ème anniversaire de l'attaque sur un couple de policiers de Magnanville	-
13 et 14 juin	Paris - AccorHotels Arena	Concert de la chanteuse colombienne Shakira	Capacité maximale 20 300 par jour
15 juin	Ensemble du Territoire	Aïd el-Fitr (fête musulmane célébrant la fin du jeune du Ramadan)	-
Mi à fin juin	Ensemble du Territoire	Epreuves du baccalauréat	-
16 juin	Ensemble du Territoire	Coupe du monde de football : France -Australie	-
16 juin	Paris - AccorHotels Arena	Concert du chanteur américain Lenny Kravitz	Capacité maximale 20 300
16 et17 juin	Le Mans	Les 24 Heures du Mans	260 000 (chiffre 2017)
21 juin	Ensemble du Territoire	Fête de la musique	-
21 juin	Ensemble du Territoire	Coupe du monde de football : France - Pérou	-

2. Evaluation de la menace terroriste

2.1. Généralités

La menace portée par les organisations terroristes demeure très élevée en France et contre nos ressortissants et intérêts à l'étranger.

2.2. Evaluation de la menace terroriste sur le territoire national

En dépit de la disparition presque complète de ses emprises territoriales en zone syro-irakienne la menace d'attaques commanditées par l'Etat islamique perdure.

Les « revenants » pourraient représenter une menace à moyen terme. Plus de 500 mineurs de moins de 15 ans, emmenés sur zone par leurs parents ou nés sur place, seraient présents en zone levantine. Avec les femmes, ils représentent près des deux tiers des Français dans cette zone de djihad. Leur retour en France constitue un vecteur potentiel de radicalisation et une menace.

Les cibles visées semblent déterminées sur des critères d'opportunités.

- les représentants de l'autorité (policiers, militaires, personnels pénitentiaires) par leur importance symbolique ;
- les lieux à forte fréquentation (centres commerciaux, transports publics, sites touristiques) ;
- les lieux de divertissement (stade, salles de concert, restaurants, cinémas) ;
- les bâtiments publics (services publics, édifices religieux, locaux associatifs ou politiques, écoles et universités, laboratoires établissements de recherche, etc.).

Enfin, le mois de mai, par ses nombreux ponts, doit être considéré avec la plus grande attention au regard des déplacements et de la hausse de fréquentation dans les transports.

2.3. Modes opératoires principaux

Si **les modes opératoires sommaires sont les plus récurrents**, un attentat complexe, nécessitant d'importants moyens, tant humains que matériels, ne doit donc pas être sous-estimé.

Les armes les plus fréquemment utilisées sont :

- les armes blanches ou autres moyens sommaires (marteaux, machettes, etc) ;
- les attaques au véhicule-bélier ;
- le recours aux engins explosifs improvisés à base de TATP ou de matières inflammables (bouteilles de gaz, combustibles liquides). Les attentats manqués des métros de Londres, le 15 septembre 2017 et de New-York, le 11 décembre 2017, démontrent que cette menace reste d'actualité.

D'autres modes opératoires pourraient émerger en fonction des préconisations de la propagande.

2.4. La menace terroriste contre les ressortissants et les intérêts français à l'étranger (IFE)

Au-delà des frontières européennes, la menace terroriste demeure particulièrement élevée à l'encontre des intérêts et des ressortissants français dans les régions de l'arc de crise (Sahel, région du lac Tchad, Afrique du Nord, Turquie, Proche et Moyen-Orient) ainsi qu'à leur périphérie.

Les représentations nationales à l'étranger (ambassades, résidences officielles, consulats, instituts, lycées et écoles françaises, emprises militaires) constituent des cibles à haute valeur symbolique pour les groupes armés terroristes. La menace d'agression ou d'enlèvements d'occidentaux demeure, notamment sur les sites les plus fréquentés par les expatriés et les touristes (sites touristiques, hôtels, restaurants, etc.) situés dans des pays régulièrement aux prises avec les partisans de *Daech*.

3. Adaptation et axes d'effort de la posture Vigipirate « *Printemps 2018* »

La posture VIGIPIRATE « *Printemps 2018* » est active à partir du 1er mars 2018 et s'applique, sauf événement particulier, jusqu'au 13 juin 2018. L'ensemble du territoire national est maintenu au niveau « *sécurité renforcée-risque attentat* ».

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

Une attention particulière sera portée aux évolutions du contexte juridique susceptibles d'intervenir au cours de la période couverte par cette posture VIGIPIRATE et rappelées dans le courrier accompagnant la présente posture.

3.1. Sécurité des établissements scolaires, universitaires et d'accueil collectif de mineurs (ACM)

Les responsables d'établissements scolaires et de l'enseignement supérieur renforcent :

- les échanges d'informations avec les préfectures conformément à l'instruction du 12 avril 2017 ;
- la coopération avec les forces de sécurité intérieure afin d'optimiser par des exercices la mise en sécurité et en sureté des établissements ;
- la protection face aux attaques cybernétiques en appliquant la *politique de sécurité des systèmes d'information de l'Etat* (PSSIE).

Une surveillance accrue des matériaux et produits sensibles est recommandée pour détecter rapidement les vols ou disparitions. Il conviendra de mettre à jour les inventaires, notamment dans les universités ou les laboratoires mixtes de recherche qui en détiennent.

Lors des voyages scolaires à l'étranger, les organisateurs se conforment aux consignes préconisées par le ministère de l'Europe et des Affaires étrangères (*Cf.* § 5.4).

Par ailleurs, l'accueil d'étudiants étrangers sur les campus universitaires peut donner lieu, en cas de comportement inapproprié, à un signalement via le *centre national d'assistance et de prévention de la radicalisation* (CNAPR) :

Appeler numéro vert :0 800 005 696

Formulaire en ligne http://www.stop-djihadisme.gouv.fr ou https://www.internet-signalement.gouv.fr

En outre, les responsables des accueils collectifs de mineurs veilleront à maintenir leurs efforts en matière de sécurisation de leurs sites tout en maintenant un niveau de vigilance élevé lors de leurs déplacements. Durant les périodes de vacances scolaires notamment, ils éviteront les regroupements de longue durée sur la voie publique ou aux abords des gares.

3.2. Vigilance lors de voyages ou de séjours à l'étranger

Il est recommandé aux Français souhaitant voyager ou séjourner à l'étranger de se connecter, avant leur départ, au site https://www.diplomatie.gouv.fr, afin de :

- consulter les fiches conseils aux voyageurs, y recueillir les numéros utiles et les conserver pendant toute la durée de leur séjour ;
- s'inscrire parallèlement sur l'application Ariane, quelle que soit leur destination, y compris à l'intérieur de l'Union européenne. Cette précaution permet :
    - de recevoir des recommandations de sécurité par courriels si la situation dans le pays le justifie ;
    - d'être contacté en cas de crise dans le pays de destination ;
    - de prévenir, en cas de besoin, la personne contact désignée.

Par ailleurs, les Français séjournant à l'étranger doivent s'enregistrer auprès des autorités consulaires afin d'être joignables en cas de crise et d'obtenir ainsi toutes les informations pratiques et instructions émanant de l'Ambassade de France.

3.3. Protection des emprises françaises à l'étranger

Au regard du niveau actuel de la menace à l'étranger une attention particulière est portée en liaison avec les autorités locales à la protection et à la surveillance des emprises françaises à l'étranger (ambassades, résidences officielles, consulats, instituts, lycées et écoles français).

4. Efforts de communication

Il est demandé de vérifier l'affichage des logogrammes « Sécurité renforcée - risque attentat ».

En effet, dix mois après la modification des niveaux d'alerte VIGIPIRATE, d'anciens logogrammes « Alerte attentat » sont encore affichés dans certains lieux publics et peuvent être source de confusion.

Ces logogrammes peuvent être téléchargés sur le site du gouvernement http://www.gouvernement.fr/vigipirate et du SGDSN http://www.sgdsn.gouv.fr/vigipirate .

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. Ces fiches sont accessibles en ligne depuis l'espace VIGIPIRATE du site Internet du SGDSN qui sera mis à jour dès l'activation de cette posture afin d'intégrer les éléments de sensibilisation propres à la période couverte.

- Annexe 1 : « *Prévention et signalement des cas de radicalisation* »
- Annexe 2 : « *Recommandations pour la sécurisation des lieux de rassemblement ouverts au public* »
- Annexe 3 : « *Sécurité du numérique – Sensibilisation des dirigeants* »

Par ailleurs, un ensemble de guides de bonnes pratiques, à destination, est mis à disposition sur le site du gouvernement http://www.gouvernement.fr/vigipirate et du SGDSN http://www.sgdsn.gouv.fr/vigipirate .

5. La sécurité des systèmes d'information

Une vigilance constante est à porter sur les systèmes d'information. L'application des mesures précisées en annexe 3, « *Sécurité du numérique – Sensibilisation des dirigeants* » doit permettre de faire face aux menaces cyber.

Hormis le jour de la commémoration du génocide arménien (24 avril 2018) pouvant donner lieu à des actions de revendication se matérialisant dans le cyber espace par des défigurations de sites web et des attaques en déni de service, **la période considérée n'est pas marquée par des événements pouvant générer un risque d'attaque informatique majeure**.

Il appartient aux organismes de surveiller leurs propres sites et de s'assurer de l'application des mesures proposées dans les guides d'hygiène informatique consultables sur les sites internet de l'ANSSI, https://www.ssi.gouv.fr/.

RESSOURCES DOCUMENTAIRES

I. Guides de bonnes pratiques et des référentiels adaptés aux secteurs d'activités des ministères sociaux disponibles et téléchargeables sur Internet

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

- http://www.interieur.gouv.fr/actualuites/L-actu-du-Ministère/Publication-du-guide-gérer-la-surete-et-la-securite-des-evenements-et-sites-culturels
- http://solidarites-sante.gouv.fr/IMG/pdf/guide_securisation_batiments.pdf

II. Etablissements d'accueil du jeune enfant et établissements relevant de la protection de l'enfance

Les gestionnaires de site pourront s'appuyer sur les mesures préconisées dans les guides de bonnes pratiques à destination des chefs d'établissement et des directeurs d'école :
- http://www.gouvernement.fr/reagir-attaque-terroriste
- http://www.education.gouv.fr/vigipirate

Ainsi que sur le guide « Sûreté dans les établissements d'accueil du jeune enfant, se préparer et faire face aux situations d'urgence particulière » (avril 2017).
- http://www.egalite-femmes-hommes.gouv.fr/wp-content/uploads/2017/04/FINAL_mise-a-jour_24-avril_guide-Securite_EAJE.pdf

- http://solidarites-sante.gouv.fr/IMG/pdf/final_mise-a-jour_24-avril_guide-securite_eaje.pdf

III. Accueils collectifs de mineurs

Les organisateurs, directeurs et animateurs en charge d'accueils collectifs de mineurs à caractère éducatif pourront s'appuyer sur les mesures préconisées dans :
- le guide vigilance attentats les bons réflexes : « accueil collectifs de mineurs » à destination des organisateurs, des directeurs et des animateurs en charge d'accueils collectifs de mineurs à caractère éducatif (janvier 2017) ;

- http://www.jeunes.gouv.fr/actualites/zoom-sur/article/guide-vigilance-attentats-accueil
- les mesures générales de vigilance, de prévention et de protection :
- http://www.gouvernement.fr/reagir-attaque-terroriste

.

ANNEXES

Annexe 1 : « *Prévention et signalement des cas de radicalisation* »

Diffusion sans restriction

Annexe 2 : « *Recommandations pour la sécurisation des lieux de rassemblement ouverts au public* »

Diffusion sans restriction

Annexe 3 : « *Sécurité du numérique – Sensibilisation des dirigeants* »

Diffusion sans restriction

Annexe 4 : « *Posture Vigipirate Printemps 2018_Mesures publiques* »

Diffusion sans restriction

Nota Bene : Une annexe complémentaire, classifiée Diffusion Restreinte, vous est par ailleurs transmise par le canal de vos RRSSI.

Annexe 1

Diffusion sans restriction

(version numérique disponible sur les sites Internet du SGDSN et du gouvernement)

PRÉVENTION ET SIGNALEMENT DES CAS DE RADICALISATION DJIHADISTE

La radicalisation djihadiste se caractérise par un changement de comportement qui peut conduire certaines personnes à l'extrémisme ou au terrorisme. L'objectif du signalement au *centre national d'assistance et de prévention de la radicalisation* (CNAPR) est de protéger, non seulement ces personnes contre elles-mêmes en s'assurant qu'elles ne sont pas sur une voie qui conduit à commettre un acte criminel, mais également la population contre de possibles comportements violents.

1 Pourquoi signaler un cas de radicalisation ?

La radicalisation djihadiste conduit à participer à des actes terroristes dans le but revendiqué de tuer de nombreux citoyens français sans distinction, en raison uniquement de leurs valeurs et de leurs modes de vie.

On parle de **processus de radicalisation** progressif avec adhésion à une idéologie avec des composantes de violence et de rupture avec l'environnement habituel. Il peut être dangereux de sous-estimer la rapidité du passage aux paliers ultimes. **La radicalisation apparaît comme un phénomène profondément lié à l'exploitation de conflits d'identité, de frustrations ou de fragilités.** Certains groupes terroristes djihadistes cherchent notamment à enrôler des individus en perte de repères et vulnérables.

La force d'une idéologie et son pouvoir d'attraction ne doivent pas être sous-estimés. Des individus ayant développé une haine de notre société peuvent adhérer pleinement à un discours qui donne sens à leurs frustrations ou à un sentiment d'humiliation, à leurs difficultés et apporte des solutions.

Cette radicalisation est un phénomène complexe, protéiforme, amplifié par le développement d'internet et des réseaux sociaux. La propagande véhiculée touche des profils variés : délinquants, personnes vulnérables en quête d'identité, personnes ayant des troubles du comportement adaptatif, etc. La complexité du phénomène actuel porte sur l'identification du niveau de radicalisation et de ses conséquences : l'ensemble des pratiquants rigoristes d'une religion ne sont pas djihadistes mais tous les djihadistes sont radicalisés.

Difficile à repérer et à traiter, la radicalisation est donc un enjeu majeur de sécurité nationale et de survie pour notre société.

2 Identifier une situation de radicalisation

Appliquer strictement les préceptes d'une religion ne constitue pas un élément alarmant en soi. La pratique religieuse doit alerter l'entourage quand elle s'accompagne pour l'intéressé, d'une volonté de rupture avec sa propre personnalité antérieure et donc, avec son entourage proche et tout ce qui peut le ramener à sa vie d'avant.

Aussi, identifier un processus de radicalisation ne se fait pas sur la base d'un seul indice. Pris isolément, un des comportements listés ci-dessous ne signifie pas qu'il y a radicalisation. **C'est la combinaison de plusieurs signes qui donne une forme de cohérence et qui doit provoquer vigilance et alerte.**

Certaines combinaisons de comportements ou de traits de caractère sont des signaux tangibles de radicalisation et doivent attirer votre attention, que ce soit dans votre environnement quotidien ou sur votre lieu de travail.

COHÉRENCE → VIGILANCE → SIGNALEMENT

- Changements physiques, vestimentaires et alimentaires ;
- Propos asociaux ;
- Passage soudain à une pratique religieuse hyper ritualisée ;
- Rejet de l'autorité et de la vie en collectivité ;
- Rejet brutal des habitudes quotidiennes ;
- Repli sur soi ;
- Haine de soi, rejet de sa propre personne, déplacement de la haine de soi sur autrui ;
- Rejet de la société et de ses institutions (école, etc.) ;
- Éloignement de la famille et des proches ;
- Modification soudaine des centres d'intérêt ;
- Appréhension complotiste, antisémite, apocalyptique de la société.

PRÉVENTION ET SIGNALEMENT DES CAS DE RADICALISATION DJIHADISTE

3 Initier une démarche de signalement

Il s'agit de prévenir, voire d'éviter, le basculement vers un comportement violent, en accompagnant les radicalisés et leurs familles par des professionnels, sous la supervision des cellules adaptées au sein des préfectures de leur département de résidence.

En signalant, on protège non seulement l'intéressé en lui évitant de participer à un acte criminel (pour le sortir au plus tôt du chemin mortifère sur lequel il s'est engagé peut-être sans en avoir conscience) **mais également la société contre de possibles préméditations de meurtres.** Prévenir c'est protéger. **Appeler ne représente pas une mesure punitive, il s'agit d'une mesure préventive.** Après un appel, les services de l'État s'appuient sur des spécialistes pour en évaluer le bien-fondé et le danger potentiel. Ils mettront en place un accompagnement adapté pour éviter que la situation ne se détériore.

Dans quels cas appeler ?

- Pour signaler une situation inquiétante, qui paraît menacer un proche ;
- Si vous avez un doute ou des questions sur une situation ;
- Pour obtenir des renseignements sur la conduite à tenir ;
- Pour être écouté(e), conseillé(e) dans vos démarches.

Appeler le numéro vert : **0 800 005 696**
Les appels sont strictement confidentiels, votre identité ne sera pas dévoilée.
Remplir le formulaire en ligne : **http://www.stop-djihadisme.gouv.fr**

4 Que se passe-t-il après un signalement ?

Si la situation est jugée préoccupante par les services de l'Etat, la personne faisant l'objet du signalement ainsi que sa **famille bénéficieront d'un accompagnement spécialisé et adapté à leur situation.**

Votre identité ne sera pas dévoilée, les signalements sont strictement confidentiels. Même si vous n'êtes pas sûr d'avoir reconnu des combinaisons de signes de comportement suspect, **vous pouvez sauver des vies.** il est donc préférable d'appeler rapidement le numéro vert. Des spécialistes se chargeront de qualifier la situation de préoccupante ou non.

Signaler une situation ne vous sera jamais reproché. Faites le avant qu'il ne soit trop tard.

5 Signaler un contenu appelant à la haine ou faisant l'apologie du terrorisme sur Internet

Internet et les média sociaux favorisent la diffusion d'appels à la haine et de messages faisant l'apologie du terrorisme.

La liberté d'expression est un élément fondamental de notre société. Elle ne constitue toutefois pas un « passe-droit » pour tout rédiger et publier n'importe quoi sur Internet. En 2009, la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation, également appelée PHAROS, a été mise en place par l'Etat pour signaler les comportements illicites sur internet.

Lorsque vous constatez des contenus appelant à la haine ou faisant l'apologie du terrorisme sur Internet, ne les partagez pas, ne les likez pas, ne les retweetez pas. Ayez le bon réflexe, signalez les sur :

https://www.internet-signalement.gouv.fr

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, déplacements, image – DSAF/DPL – Février 2018.

Annexe 2

Diffusion sans restriction

(version numérique disponible sur les sites Internet du SGDSN et du gouvernement)

RECOMMANDATIONS POUR LA SÉCURISATION DES LIEUX DE RASSEMBLEMENT OUVERTS AU PUBLIC

(Fiche actualisée en date du 2 février 2018)

Cette fiche traite de la protection des lieux de rassemblement ouverts au public (événements sportifs, festivals, marchés de Noël, braderies, etc.) et doit pouvoir servir de guide pratique aux organisateurs de ce genre de manifestations. Elle doit être largement diffusée. Certains des conseils délivrés ci-dessous peuvent ne pas être applicables à tous les sites. Ils doivent donc être adaptés en fonction de la configuration des lieux et du bon sens de circonstance.

1 Identifier les menaces et les vulnérabilités

Il faut d'abord évaluer la sensibilité du rassemblement en lien avec les autorités locales (préfet, maire, Police Nationale, Gendarmerie Nationale) :

- pourquoi ce rassemblement pourrait-il être ciblé par des terroristes ?
- en quoi est-il un symbole du mode de vie occidental et des valeurs de la République ?
- ce rassemblement a-t-il une couverture médiatique qui donnerait une forte visibilité à une action terroriste ?

Les différentes attaques possibles doivent être envisagées :

- jet ou dépôt d'un engin explosif à l'intérieur ou en périmétrie du site ;
- véhicule piégé en stationnement aux abords du site ;
- véhicule-bélier ;
- fusillade ou attaque suicide ;
- prise d'otage ;
- attaque à l'arme blanche.

2 Organiser la sécurité de l'événement

Il est primordial que les organisateurs de rassemblements se coordonnent avec le maire et le préfet, ainsi qu'avec les forces de police, de gendarmerie, les services de police municipale et d'incendie et de secours.

Par ailleurs, il peut être nécessaire de faire appel aux compétences de sociétés privées de sécurité pour renforcer la sécurité d'un tel événement.

2.1 - En périphérie du rassemblement

- **choisir le lieu d'implantation de l'événement qui présentera le moins de vulnérabilités.** Il est préférable de choisir le lieu du rassemblement de manière à limiter l'accès de véhicules (ne pas s'installer au débouché d'un axe important) ;
- **limiter ou interdire le stationnement** des véhicules aux abords immédiats du lieu du rassemblement ;
- **mettre en place une signalétique** afin d'orienter les piétons sur le lieu de l'événement et de détourner les flux de véhicules ;
- **cloisonner le flux des véhicules de l'espace de déambulation des piétons ;**
- **identifier le mobilier urbain** qui pourrait servir à dissimuler de l'explosif, le faire retirer par les autorités habilitées, en réduire l'utilisation ou mettre en place des rondes de vérification ;
- **solliciter les forces de l'ordre** ou la police municipale pour la réalisation de patrouilles, voire la mise en place de points de contrôle et de filtrage. Des agents des sociétés privées de sécurité peuvent concourir à cette mission ;
- **identifier les points de vulnérabilité hauts** (immeubles surplombant) et les sécuriser, éventuellement par une présence humaine ;
- si possible, mettre en place un système de vidéoprotection donnant, en priorité, sur les accès au site, en prenant en compte les dispositions du Code de la sécurité intérieure.

RECOMMANDATIONS POUR LA SÉCURISATION DES LIEUX DE RASSEMBLEMENT OUVERTS AU PUBLIC

(Fiche actualisée en date du 2 février 2018)

2.2 - Sur la périmétrie du rassemblement

- **aménager des points de contrôle ou de filtrage en nombre suffisant** aux entrées du site afin de fluidifier l'entrée du public. Leur efficacité repose sur la présence d'un superviseur, de moyens de communication et de procédures claires afin de diffuser l'alerte et de faciliter l'intervention des forces de sécurité intérieure en cas d'incident ;
- **maintenir le niveau de vigilance tout au long de l'événement mais également lors du moment sensible de sa dispersion** (le 22 mai 2017 à Manchester, au Royaume-Uni, un homme a fait détoner une charge explosive qu'il portait sur lui à la sortie de la salle de spectacle *Manchester Arena*), en rappelant régulièrement des messages de sensibilisation à destination du public (*via* la sonorisation de l'événement par exemple – « TOUS acteurs de la sécurité) » ;
- **installer une délimitation physique du périmètre extérieur** de l'événement au moyen de barrières reliées entre elles, de blocs en béton, de véhicules du comité d'organisation comme élément de barrage, etc. ;
- organiser un ou plusieurs cheminements jusqu'au point de contrôle en installant des barrières. Séparer, dans la mesure du possible, les flux entrants et les flux sortants ;
- **aménager les issues de secours en nombre suffisant** au regard de l'importance de l'événement afin de permettre une évacuation rapide du public en cas de danger à l'intérieur de la zone ;
- **organiser et contrôler les livraisons.** Prévoir des équipements mobiles permettant de bloquer physiquement les véhicules appelés à pénétrer dans le périmètre le temps de ce contrôle ;
- apposer les affiches de sensibilisation à destination du public aux points d'entrées notamment « Réagir en cas d'attaque terroriste ».

Les véhicules-béliers constituent un mode d'action terroriste de plus en plus utilisé : attentats de Nice et de Berlin en 2016, attaque contre une patrouille de militaires à Levallois-Perret, attentats en Catalogne et attaque au camion-bélier à New-York en 2017. Pour faire face à ce mode opératoire, il est recommandé de mettre en place des moyens de circonstance permettant d'interdire l'accès au site ou de réduire la vitesse des véhicules à proximité des lieux de rassemblement. La mise en place de chicanes avec des obstacles successifs est également conseillée : plots en béton, bacs de fleurs de dimensions importantes, herses mobiles, barrières d'arrêt ou véhicules lourds (camions). Il est indispensable de tenir compte de la distance de pénétration potentielle d'un véhicule-bélier lors de la définition du périmètre extérieur d'un rassemblement (distance de sécurité entre les dispositifs de sécurité et la foule).

2.3 - Au niveau des volumes intérieurs

- **désigner un responsable sûreté** qui sera l'interlocuteur unique des forces de l'ordre et des services d'incendie et de secours en cas d'intervention sur le site. Véritable coordinateur de la sûreté de l'événement, il doit connaître les bons réflexes à adopter. Il peut se rapprocher préalablement des forces de sécurité intérieure pour recueillir leurs conseils ;
- prévoir l'aménagement d'un **poste central de sûreté** au sein du site. Ce dernier doit être équipé 24H/24 par au moins un opérateur en mesure de visualiser les images du système de vidéo-protection mis en place ;
- **sécuriser la zone en période de fermeture du public** par la mise en œuvre d'un gardiennage humain ;
- **sensibiliser l'ensemble des collaborateurs au niveau de menace,** aux modes opératoires terroristes et à la détection de situations suspectes. Cette sensibilisation doit être complétée par une information sur les comportements à adopter en cas d'attaque.

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, déplacements, image – DSAF/DPL – Février 2018.

Annexe 3

Diffusion sans restriction

(version numérique disponible sur les sites Internet du SGDSN et du gouvernement)

SÉCURITÉ DU NUMÉRIQUE
SENSIBILISATION DES DIRIGEANTS

Cette fiche s'adresse aux dirigeants d'entreprises privées ou de collectivités territoriales et vise à les aider à appréhender la question de la sécurité du numérique à travers quelques exemples et recommandations pratiques.

1 Cela pourrait vous arriver…

Les scénarios proposés ci-dessous illustrent quelques exemples (parmi d'autres) de menaces de nature cyber pesant sur les organisations et relevant de la responsabilité de leurs dirigeants.

Usurpation d'identité / hameçonnage

Le hameçonnage consiste à usurper l'identité de l'expéditeur dans le but de duper le destinataire qui est invité à ouvrir une pièce-jointe malveillante ou à suivre un lien vers un site Web malveillant. Une fois cette 1ère machine contaminée, l'attaquant en prend le contrôle pour manœuvrer au sein du système d'information de l'organisation.

Arnaud reçoit une demande d'ajout de contact sur LinkedIn de la part de son supérieur hiérarchique pendant la période des fêtes de fin d'année. Ce dernier est en congés et souhaite lui transmettre des documents car il n'a pas accès à sa boîte mail momentanément. Mais ce qu'Arnaud ne sait pas, c'est que la personne qui s'adresse à lui n'est pas son supérieur mais un groupe d'attaquants ayant usurpé son identité. En transmettant à ce collaborateur un simple document contenant une charge malveillante, ils ont pu compromettre les équipements de l'entreprise connectés à Internet et exfiltrer des données sensibles en relation avec une importante négociation commerciale de nature confidentielle. Dès le lendemain, les informations fuitent dans la presse, conduisant ainsi à la rupture de la négociation au profit d'une entreprise concurrente.

Rançongiciel

Le rançongiciel est un programme malveillant chiffrant tout ou partie des données stockées sur un ordinateur ou accessibles par un réseau. L'objectif est de proposer à la victime de récupérer ses données en échange du paiement d'une rançon.

Guillaume est dirigeant d'entreprise. Nous sommes vendredi après-midi avant le début des congés de fin d'année et Guillaume avait déjà autorisé ses employés à partir exceptionnellement à 15h00. Son responsable sécurité lui indique qu'une mise à jour de l'ensemble des postes de travail doit être réalisée mais ne pourra pas être effective avant 15h00. Guillaume décide de fermer l'entreprise comme prévu et de reporter l'opération de mise à jour.

Le 2 janvier, les ordinateurs de tous les employés affichent un écran noir porteur d'un message exigeant d'eux le paiement d'une rançon en échange de la récupération de leurs données. Les employés ne pouvant plus travailler, l'activité de l'ensemble de l'entreprise et de ses sous-traitants est à l'arrêt et mise en péril.

Les conséquences pour votre entreprise peuvent être graves :
perte financière importante, atteinte à l'image de l'organisation, etc.

2 S'emparer de la question de la sécurité numérique

5 questions pour faire le point

- Depuis quand n'ai-je pas entendu parler de cybersécurité ?
- Mon entreprise est-elle une cible d'intérêt pour des attaquants ?
- Ai-je pris toutes les précautions pour protéger mes informations et les échanges avec mes partenaires et mes collaborateurs ?
- Quel est la part du budget consacrée à la sécurité informatique ?
- Ai-je déjà parlé de cybersécurité à mes collaborateurs ?

5 questions à poser à mon RSSI

- Quelles sont nos principales vulnérabilités ?
- Quels sont les moyens de protection actuellement en place pour lutter contre les attaques et codes malveillants ?
- A-t-on déjà fait un audit de sécurité des SI ?
  A-t-on déjà fait une analyse de risques ?
  Dispose-t-on d'une cartographie des SI ?
- Sommes-nous préparés si une crise d'origine cyber survenait ?
- Disposons-nous d'une couverture juridique et nos contrats d'assurance intègrent-ils le risque cyber ?

SÉCURITÉ DU NUMÉRIQUE
SENSIBILISATION DES DIRIGEANTS

Vous êtes au cœur de la stratégie de gestion des informations clés de l'entreprise. Vos données personnelles sont autant d'informations potentiellement convoitées par des individus aux intentions malveillantes. Soyez notamment vigilant à l'égard de possibles usurpations de votre identité sur les réseaux sociaux et maîtrisez les informations sur votre entreprise qui circulent sur Internet.

Sensibiliser vos employés aux bonnes pratiques

Vos employés doivent être sensibilisés voire formés aux bonnes pratiques de l'informatique et devenir acteur de la sécurité numérique de leur entreprise.

Analyser les risques et protéger les systèmes d'information sensibles

Il est essentiel de savoir quels sont les systèmes d'information les plus cruciaux pour le bon fonctionnement de votre entreprise afin de pouvoir traiter les risques susceptibles de les fragiliser.

Préparer votre entreprise à une attaque informatique

Assurez-vous de disposer d'un plan de réaction aux incidents de sécurité (notamment un processus de sauvegarde régulier des données critiques) et testez-le. En particulier, établissez une chaine de remontée d'incidents connue des employés afin de reconnaitre au plus tôt une tentative d'attaque.

Organiser un exercice simulant une attaque

Un exercice de gestion de crise permet de vérifier la solidité des procédures mises en place dans votre organisme et de les corriger si nécessaire.

3 Vous pensez avoir été victime d'une attaque

Qui prévenir ?

Dirigeant d'une entreprise (TPE, PME) ou d'une collectivité territoriale, il est recommandé de vous rendre sur la plateforme numérique **www.cybermalveillance.gouv.fr** afin d'être mis en relation avec des prestataires de proximité susceptibles de vous assister techniquement. Vous pouvez également déposer plainte auprès d'un service de la Police nationale ou de la Gendarmerie nationale ou adresser un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent.

4 Documents de référence

Guide des bonnes pratiques de l'informatique
https://www.ssi.gouv.fr/uploads/2017/01/guide_cgpme_bonnes_pratiques.pdf.pdf
Guide d'hygiène informatique (à l'attention des DSI)
https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
MOOC (Massive Open Online Course) SecNumacadémie de l'ANSSI
https://www.secnumacademie.gouv.fr
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