NBS NESTLÉ BUSINESS SERVICES
Capturing Our Potential
Nestlé

Prévention et gestion du risque terroriste en entreprise

Mémoire sous la direction de Monsieur Patrick Thourot

présenté en vue d'obtenir le Master Manager de l'assurance

Pauline STEVANCE | Année universitaire 2017/2018

Cycle Alternant

le cnam
enass

Remerciements

Je tiens tout d'abord à exprimer toute ma gratitude à mon directeur de mémoire, Monsieur Patrick Thourot, qui a pris le temps de répondre à mes questions et de m'apporter de solides pistes de réflexion.

Mes sincères remerciements vont également à :

Madame Constance Thivend, ma tutrice, pour la qualité de son accompagnement et la confiance qu'elle m'a accordée dans le cadre de mon activité.

Monsieur Pascal Martin, Risk Manager de Nestlé France, pour son professionnalisme et sa sympathie au cours de ces deux années de Master.

Madame Isabelle Riou, assistante au sein du Département Risk Management de Nestlé France, pour son soutien et sa joie de vivre au quotidien.

A ma mère, à mon père, à mes amis, à mes coaches qui m'ont aidé à concilier sport à haut niveau, études et activité professionnelle.

A mon cousin Vincent, pour son engagement dans l'armée française et ses années passées à l'étranger à lutter contre le terrorisme et la propagation de la haine.

Sommaire

Résumé

Les risques évoluent et changent de manière considérable pour plusieurs raisons. L'une des raisons majeures de cette métamorphose des risques est le fait qu'il y ait des mises en contact de l'Homme de plus en plus conséquentes ce qui induit une augmentation accrue de la population et de la densité. Ceci sous-entend des bénéfices (gains de productivité, croissance économique) mais surtout des risques plus importants... La croissance de la population a engendré de lourds problèmes comme le terrorisme – ce risque qui serait quasi nul aujourd'hui si la population mondiale était divisée par 100. Le terrorisme n'a pas toujours existé, il n'est apparu que lorsque la population mondiale a atteint un certain seuil. Il est fondamental de s'imprégner de cette notion pour identifier et gérer le risque terroriste de manière efficace.

Au niveau des grandes entreprises, tous les actifs et les types de business sont internationalisés aujourd'hui. Ainsi, les 135 plus grandes entreprises françaises réalisent 50% de leur chiffre d'affaires à l'étranger, et surtout, ont 3,7 millions d'emplois à l'étranger. Un tiers des entreprises de taille intermédiaire[1] sous contrôle français sont situées à l'étranger. Plus frappant encore, les stocks d'investissements directs français à l'étranger représentent 45% du PIB français. Enfin, les multinationales françaises détiennent 40.000 filiales à l'étranger et y réalisent 53,3% de leur chiffre d'affaires.[2]

Ces constats mettent en exergue les forts mouvements de population et expliquent l'accroissement du risque terroriste : avec la mondialisation, il y a davantage de voyageurs et d'expatriés. Au quotidien, pour une multinationale – comme Nestlé – cela représente plus de 10.000 collaborateurs transportés collectivement chaque jour, quel que soit le mode de transport. Le risque terroriste pèse lourd sur l'acteur économique qu'est l'entreprise. L'entreprise française représente la France et est signe de richesse et d'argent, ce qui en fait une cible majeure pour les terroristes. Aussi, il convient de noter que sur la scène internationale et géopolitique, la France – comme les autres grandes puissances occidentales – est impliquée dans des conflits sur des « territoires émergents » ; ce qui renforce sans nul doute son exposition au terrorisme.

[1] Appelées communément « ETI »
[2] Données chiffrées issues du rapport INSEE 2016

Glossaire

- terrorisme

- cyber-attaque

- résilience

- risk management

- sûreté

- sécurité

- cartographie

- entreprises

- radicalisation

- menace

- risque

- prévention

- protection

- cellule de crise

- assurance

Introduction

« Un attentat reste un attentat. A l'usure, on peut le gérer techniquement, pas humainement. L'émoi et l'effroi ne font pas bon ménage avec le sang-froid. Lorsque l'horreur frappe, c'est toujours le cœur qu'elle vise en premier. »

Yasmina Khadra

Le terrorisme est défini de la manière suivante : « ensemble d'actes de violence (attentats, prises d'otages, etc.) commis par une organisation ou un individu pour créer un climat d'insécurité, pour exercer un chantage sur un gouvernement, pour satisfaire une haine à l'égard d'une communauté, d'un pays, d'un système ».[3]

Les réseaux terroristes agissent depuis des décennies. Mais à l'heure de la digitalisation et des modes de communication en multicanal, la menace évolue. En France, l'état d'urgence est prolongé – pour la sixième fois – jusqu'au 1er novembre 2017. Ce contexte inédit, et surtout anxiogène, a lourdement impacté les méthodes de gestion et de prévention des risques en entreprise. La législation en vigueur, et notamment l'obligation de sécurité légale de l'employeur, engage les entreprises à considérer les menaces externes. Cependant, selon les secteurs d'activités, les seuils de vigilance fixés sont plus ou moins importants. En effet, le transport de personnes, la chimie ou encore le nucléaire, restent des secteurs particulièrement sensibles en cas d'attentat ; sans nul doute en raison de la gravité exceptionnelle des conséquences humaines et matérielles que peuvent représenter ces attaques. C'est dans le cadre de la continuité d'activité que l'on retrouve des méthodes communes entre les différentes branches professionnelles. Par exemple, le risque de désorganisation et son sous-jacent, le droit de retrait du salarié. Il s'agit ici de notions qui inquiètent l'ensemble des sociétés françaises. Le droit de retrait[4] accorde au salarié la possibilité de cesser son activité s'il juge que la situation présente un danger grave et imminent pour sa vie ou sa santé, ou qu'il ressent une défectuosité dans le système de protection. C'est là que peuvent intervenir transversalement les techniques et produits

[3] Source : Dictionnaire Larousse
[4] Source : Article L-4131-1 du Code du travail

assuranciels, notamment l'assurance « homme-clé ». Cette possibilité favorise le maintien de l'activité. Or, existe-t-il des limites de garantie en cas d'absence de collaborateurs émanant d'une menace terroriste ? C'est bien évidemment l'anticipation du risque terroriste, et des problématiques qui en découlent, qui reste la meilleure façon de gérer ce risque.

Les Risk Managers et les Directions Sécurité et Sureté des entreprises privées se dotent de nouveaux moyens, de nouvelles méthodes pour faire face à ce risque majeur. L'appréhension du risque terroriste passe notamment par la formation des collaborateurs et la mise en place de dispositifs de protection. En amont comme en aval, la menace est abordée avec prudence, le sujet – presque devenu tabou du fait des événements terribles survenus en 2015 et 2016 – est traité en petit comité au sein des entreprises du secteur privé. Est-ce là la manière optimale de maîtriser ce risque ? Les Risk Managers disposent-ils de connaissances et compétences suffisantes pour se voir octroyer la gestion de ce risque ? Peuvent-ils devenir les premiers interlocuteurs de l'entreprise en lien avec les forces de l'ordre ?

Sous un angle plus global, **quelles sont les méthodes les plus efficientes pour répondre à une complexification du risque terroriste** ?

Afin d'étudier le sujet de manière exhaustive, il convient tout d'abord d'identifier la place du risque terroriste dans la cartographie des risques de sécurité et de sûreté puis de définir les solutions nouvelles permettant de gérer ce risque.

Partie 1 : Le terrorisme, risque majeur dans la cartographie des risques de sûreté en entreprise

A] L'IMPACT DES ATTENTATS TERRORISTES SUR LES ENTREPRISES

1) La cartographie des risques sécuritaires

a- Définition

Etymologiquement, le mot terrorisme est issu du latin *terror*, qui signifie la terreur. Ce terme était autrefois utilisé pour décrire des situations de guerre ou d'extermination des hommes. Le mot terrorisme est donc intrinsèquement violent et détient des connotations liées à la peur, à la guerre et à la barbarie. Le terrorisme a toujours existé et existera – a priori – toujours, mais sous des formes différentes.

Il convient de rappeler qu'à l'origine, le terrorisme était une action de l'Etat avec, historiquement, la période de la Terreur (avec la lettre t en majuscule). La Terreur se caractérisait par des exécutions de masse et des massacres ; cela remonte à 1793 en France. Depuis cette période, un changement de paradigme a été observé quant à la terreur et au terrorisme. C'est à partir du XIXe siècle que le terrorisme devient non plus une action de l'Etat mais une action contre l'Etat et ses représentants. En frappant une entreprise ou des civils, c'est avant tout le pays qui est frappé par le terroriste. *De facto*, ce qui caractérise par-dessus tout le risque terroriste est le fait qu'il soit provoqué par l'action de l'Homme. C'est en cela qu'il est totalement distinct des autres risques qui peuvent être couverts de nos jours par les produits et garanties assurantiels, les captives ou encore les marchés financiers.

Même si les dictionnaires apportent des définitions du terrorisme, peu sont précises et objectives. En effet, le terrorisme évolue sans cesse et n'est pas le même selon les pays concernés, les raisons pour lesquelles les terroristes agissent, ou l'histoire de la zone touchée par l'attentat. Quoiqu'il en soit, le risque terroriste montre toujours les mêmes caractéristiques : c'est un acte violent réalisé dans un contexte de paix qui a pour objectif d'imposer la terreur aux civils. Les raisons clamées par les terroristes sont liées à la religion, la politique ou toute autre forme d'idéologie. C'est un genre nouveau de guerre qui sème le doute parmi toutes les instances et déstabilise de nombreux experts.

En ce qui concerne l'assurance du risque terroriste, la création, la mise en place et la gestion des produits couvrant ce risque nécessite un traitement très particulier. Ce risque exige une mutualisation singulière et une approche globale à long terme. Parce qu'il peut se développer très vite et outrepasser toutes les formes d'attentats que l'on connaît déjà, il est fondamental de maîtriser ce risque en mobilisant tant les assureurs que l'Etat, les entreprises et l'ensemble des acteurs économiques du pays. Le terrorisme surprend toujours et se développe là où il n'est pas attendu.

La problématique majeure du terrorisme résulte du fait qu'il s'agisse d'un risque pouvant se déployer à l'échelle planétaire. On parle fréquemment d'hyper-terrorisme lorsque plusieurs pays ou plusieurs zones sont touchés. C'est un risque dont la probabilité d'occurrence reste relativement faible au niveau de la France et de l'Europe. En revanche, c'est un risque dit « sensible » puisque les médias relaient beaucoup d'informations à ce sujet aujourd'hui. Les citoyens et la Société (au sens large) sont très sensibles à ce type d'événement.

Ce risque peut aussi devenir extrême s'il emploie des moyens de destruction massive en s'attaquant notamment aux domaines du nucléaire, de la bactériologie, de la radiologie ou de la chimie. Ces activités sont en effet particulièrement exposées et les entreprises qui œuvrent dans ces domaines en sont conscientes. Les politiques de sûreté de ces entreprises sont souvent très développées et depuis longtemps. Mais compte-tenu de la vitesse d'évolution du terrorisme au cours des dernières années, le risque de destruction massive est toujours envisageable et ne doit pas être écarté.

Les nouvelles technologies sont de plus en plus accessibles pour les organisations terroristes. Le terrorisme du XXIème siècle se basera surtout sur l'utilisation du numérique et les attaques digitales. Le cyber-terrorisme sera sans nul doute mondialisé et les entreprises et les états doivent y être préparés. Aussi, il est essentiel de rappeler que le risque terroriste existe sous de nombreuses formes et cette menace se décline de manière parfois très différente. Le cyber-terrorisme ne sera donc peut-être pas la seule forme de terrorisme qui devra être appréhendée durant les décennies à venir.

Au cours du XXe siècle, les organisations et les institutions ont été confrontées essentiellement au risque terroriste religieux et dogmatique ainsi qu'au risque terroriste individuel. Le risque terroriste religieux et dogmatique est sans doute le plus ancien mais aussi le plus difficile à maîtriser. L'origine du terrorisme religieux et dogmatique est souvent liée à une opposition aux nouveaux concepts économiques et sociaux issus de la mondialisation. Pour identifier ce risque, les connaissances et études d'experts – en théologie par exemple – sont nécessaires. Comprendre l'interprétation qui est faite des dogmes et religions par une organisation terroriste est un travail lourd et complexe ; bien que primordial pour mener des actions de lutte anti-terroriste.

Une seconde forme de terrorisme est le terrorisme individuel. Il cherche à atteindre majoritairement des « icônes » politiques, des personnages affirmant leur opinion politique et dont l'exposition et la notoriété sont importantes. Les actes terroristes des dernières années en France et en Europe ne sont pas issus du terrorisme individuel. Les terroristes « actuels » font en effet partie d'organisation pour lesquelles ils sont prêts à sacrifier leur vie.

Enfin, il existe une autre forme de terrorisme : le terrorisme d'Etat. Il s'agit d'une forme de terrorisme moins répandue. C'était d'ailleurs ce terrorisme qui était appliqué lors du régime de la Terreur en France vu précédemment. Dans les pays occidentaux, fort heureusement, ce terrorisme n'est plus observé du tout. Malgré tout, il est encore présent dans de nombreux pays aujourd'hui. En 2014, L'organisation non gouvernementale internationale Amnesty International a d'ailleurs signalé en 2014 l'application par 141 pays de multiples formes de torture et de terrorisme d'Etat. Ces derniers sont mis en œuvre par les forces de sécurité, la police ou d'autres agents de l'État[5].
Toutes ces formes de terrorisme sont aujourd'hui punies et réprimandées par les lois internationales. Qu'il s'agisse de terrorisme d'Etat, de terrorisme individuel, ou encore de terrorisme dogmatique et religieux, la barbarie et la violence faites à autrui sont dénoncés par les organisations internationales pour la défense des droits de l'Homme comme l'ONU[6].

[5] Source : Amnesty international, rapport de 2014.
[6] ONU : Organisation des Nations Unies ; dispose d'un bureau de lutte contre le terrorisme international, le « counterterrorism ».

Au niveau juridique en France, le terrorisme – sous toutes ses formes – est puni au niveau pénal. Il est défini dans le Code Pénal par les articles 421–1 et 421–2 ci-après. Les informations relatives aux conditions légales du terrorisme en France seront détaillées dans la partie traitant du rôle de l'Etat (Partie 2, encart B, 1).

Article 421-1

Modifié par LOI n°2011-266 du 14 mars 2011 - art. 18

Constituent des actes de terrorisme, lorsqu'elles sont intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur, les infractions suivantes :

1° Les atteintes volontaires à la vie, les atteintes volontaires à l'intégrité de la personne, l'enlèvement et la séquestration ainsi que le détournement d'aéronef, de navire ou de tout autre moyen de transport, définis par le livre II du présent code ;

2° Les vols, les extorsions, les destructions, dégradations et détériorations, ainsi que les infractions en matière informatique définis par le livre III du présent code ;

3° Les infractions en matière de groupes de combat et de mouvements dissous définies par les articles 431-13 à 431-17 et les infractions définies par les articles 434-6 et 441-2 à 441-5 ;

4° Les infractions en matière d'armes, de produits explosifs ou de matières nucléaires définies par le I de l'article L. 1333-9, les articles L. 1333-11 et L. 1333-13-2, le II des articles L. 1333-13-3 et L. 1333-13-4, les articles L. 1333-13-6, L. 2339-2, L. 2339-5, L. 2339-8 et L. 2339-9 à l'exception des armes de la 6e catégorie, L. 2339-14, L. 2339-16, L. 2341-1, L. 2341-4, L. 2341-5, L. 2342-57 à L. 2342-62, L. 2353-4, le 1° de l'article L. 2353-5 et l'article L. 2353-13 du code de la défense ;

5° Le recel du produit de l'une des infractions prévues aux 1° à 4° ci-dessus ;

6° Les infractions de blanchiment prévues au chapitre IV du titre II du livre III du présent code ;

7° Les délits d'initié prévus à l'article L. 465-1 du code monétaire et financier.

Source : Légifrance, code pénal.

La lutte contre le terrorisme est réalisée à toutes les échelles, par tous les acteurs économiques d'un pays. L'appréhension du terrorisme dans le cadre de l'entreprise est assez spécifique. Il faut non seulement songer aux spécificités légales mais aussi à l'impact qu'un risque peut avoir sur l'entreprise toute entière. Les Risk Manager utilisent dans un premier temps un outil appelé cartographie des risques pour pouvoir identifier un risque et le conceptualiser dans son univers. La cartographie est un outil de référence en matière de gestion des risques. Elle résulte d'une démarche globale, devenant un outil de visualisation des risques majeurs d'une entreprise à un instant « T ».

En donnant une représentation synthétique des risques majeurs à date, elle permet à l'entreprise de piloter la gestion des risques et de contribuer à sa performance. La cartographie des risques Sécurité/Sûreté est une cartographie des risques opérationnels basée sur le scénario de l'évènement redouté ou sur la menace.

Il faut avant toute chose distinguer les risques de sécurité des risques de sûreté. La sécurité provient du terme *safety* en anglais, ce qui évoque les situations accidentelles. A l'inverse, la sûreté est traduite par le mot *security* qui définit des situations intentionnelles[7]. Ajoutons à cela les termes « sécurité publique », « sécurité informatique » pour traiter des problématiques de sûreté et l'on comprend pourquoi il est nécessaire d'acter un lexique clair.

Ainsi, par convention interne au monde des entreprises, la sécurité traite des situations accidentelles, elle est donc liée à une obligation de résultats, et la sûreté traite des actes intentionnels, ce qui la lie à une obligation de moyens. Pour illustration, les risques de sécurité peuvent être liés à l'incendie, à la pollution des sols, aux accidents divers. Les risques de sûreté sont relatifs à la petite délinquance, à la protection des expatriés, à la cyber-sécurité, au terrorisme.

En clair, la sûreté représente la combinaison des mesures ainsi que des moyens humains et matériels visant à protéger les sites et l'exploitation contre les actes d'intervention illicites et de malveillance. Par opposition, la sécurité consiste à se prémunir contre des évènements ne relevant pas de l'intention de nuire, tels que des défaillances mécaniques et de situations accidentelles ou naturelles.

On comprend aisément avec ces définitions que le risque terroriste est purement un risque de sûreté et non de sécurité. Ces définitions représentent le premier échelon de la démarche de cartographie des risques. Mais l'exercice de cartographie des risque est étendu vers d'autres domaines (La finance, les ressources humaines, le marketing, etc.).

b- Cartographie et schématisation

Un agent économique, quel qu'il soit peut avoir un certain « *risk appetite* », c'est-à-dire être plus ou moins averse au risque. Il saisit le risque comme une opportunité ou bien il le transfert, le gère ou le rejette comme étant une menace. La menace est un élément négatif du risque. En matière de terrorisme, on ne peut accepter aucune part du risque.

[7] Définition donnée par Eric CONTEGAL, Responsable Audit et Risques ATMB – Autoroutes et Tunnel du Mont Blanc.

En effet, les enjeux et conséquences sont beaucoup trop importants puisque le terrorisme est fréquemment déployé sous des formes de violences très puissantes. La vie humaine est au centre de ce risque, ce qui en fait donc un risque majeur.

Cette menace terroriste en entreprise se décline soit en interne, soit en externe. Concrètement, le risque peut provenir de l'extérieur (clients, fournisseurs, individus étrangers à l'entreprise, …) ou de l'intérieur (salariés, sous-traitants…). On peut aussi catégoriser le terrorisme sous d'autres angles.

Cela peut concerner tout d'abord l'humain : le personnel, les prestataires et les clients. Ces derniers peuvent être victimes des attentats, de kidnapping, d'agressions, etc… Ensuite, la menace peut impacter les biens matériels par les vols, la piraterie, la destruction massive des biens de l'entreprise.

Enfin, c'est aussi le patrimoine immatériel qui est touché : les vols d'informations commerciales (fichiers clients…) et technologiques (ordinateurs, machines, brevets, licences…), les actifs financiers (blanchiment, chantage…), l'image et la notoriété de l'entreprise et plus précisément aujourd'hui son e-réputation sur les réseaux sociaux.

Cette menace terroriste gravite dans un univers de risque de sûreté très complexe qui comprend la sûreté des biens et des personnes, la sécurité informatique et la fraude économique. Ces risques ont un rapport avec plusieurs branches de l'entreprise. Ainsi la sécurité informatique est, de manière très logique, liée à l'IT (service informatique), la fraude économique à la finance et la sûreté des biens et des personnes essentiellement aux ressources humaines.

Selon les missions et les cas rencontrés, d'autres services peuvent être amenés à travailler conjointement sur ces typologies de risques. Or, pour le risque terroriste, tous les services de l'entreprise sont concernés en permanence. Le risque terroriste est « la face émergée de l'iceberg » puisque derrière lui se cache d'autres risques : risques dommages (incendie, vol, destructions de toutes natures), des risques sanitaires, des risques psychosociaux, du risque d'image, des pertes d'exploitation, etc…

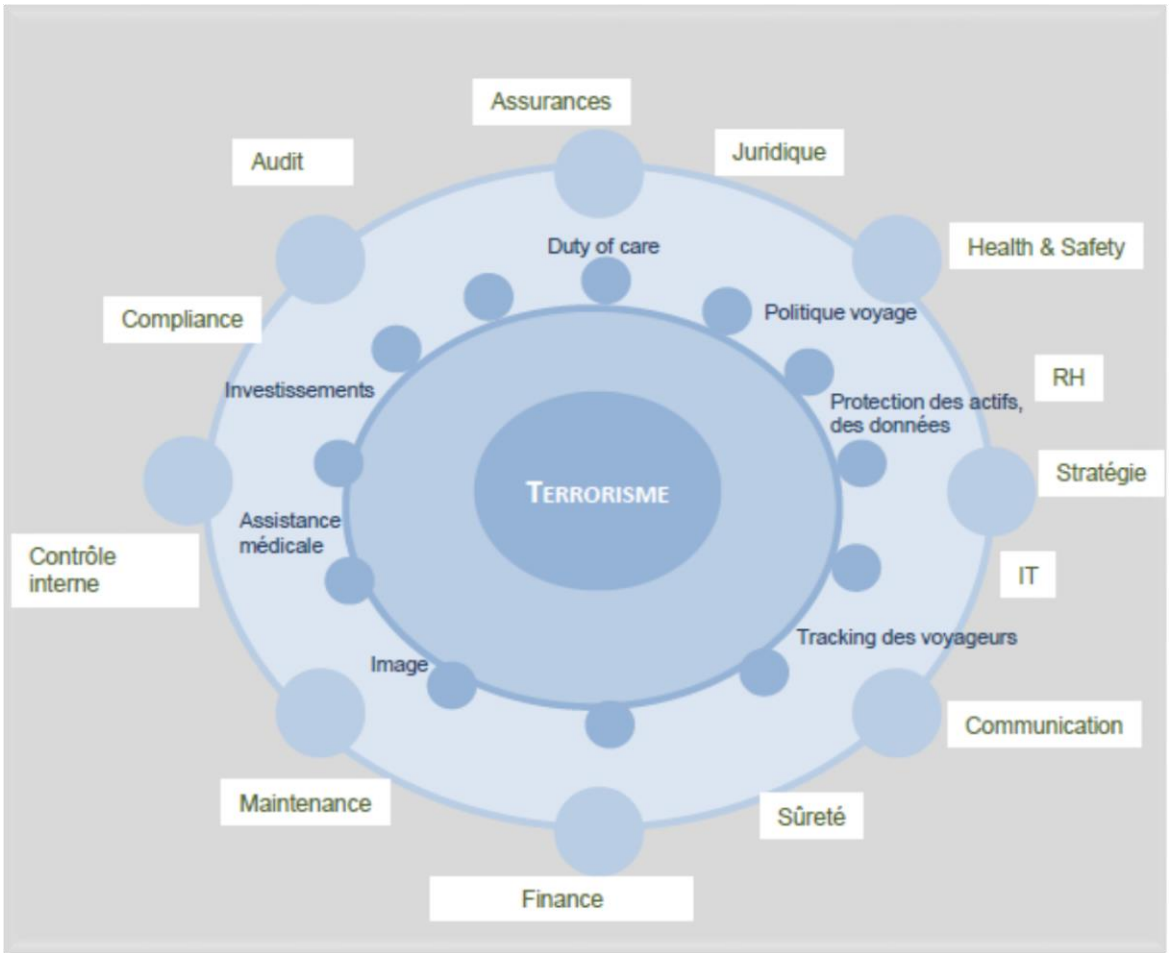
La liste est très longue et ne peut être exhaustive puisque le risque terroriste évolue sans cesse et se complexifie d'année en année.

Tout va plus vite, l'information devient de plus en plus accessible et les avancées technologiques jouent en la faveur des organisations terroristes qui attaquent désormais le monde (réel) et le monde virtuel.

Le risque terroriste se place donc au centre de tous les départements. Il peut affecter tant la Direction Sûreté/Sécurité que la Stratégie, l'Audit ou les Ressources Humaines. Mais tous les acteurs de l'entreprise sont concernés par ce risque et ont un rôle à jouer pour réduire l'exposition face à la menace. Le schéma ci-dessous illustre la dimension et les enjeux du terrorisme dans le monde de l'entreprise.

Schéma : Février 2018, réalisé par Frédéric GALLOIS

Directeur Général Délégué de GALLICE Protection.

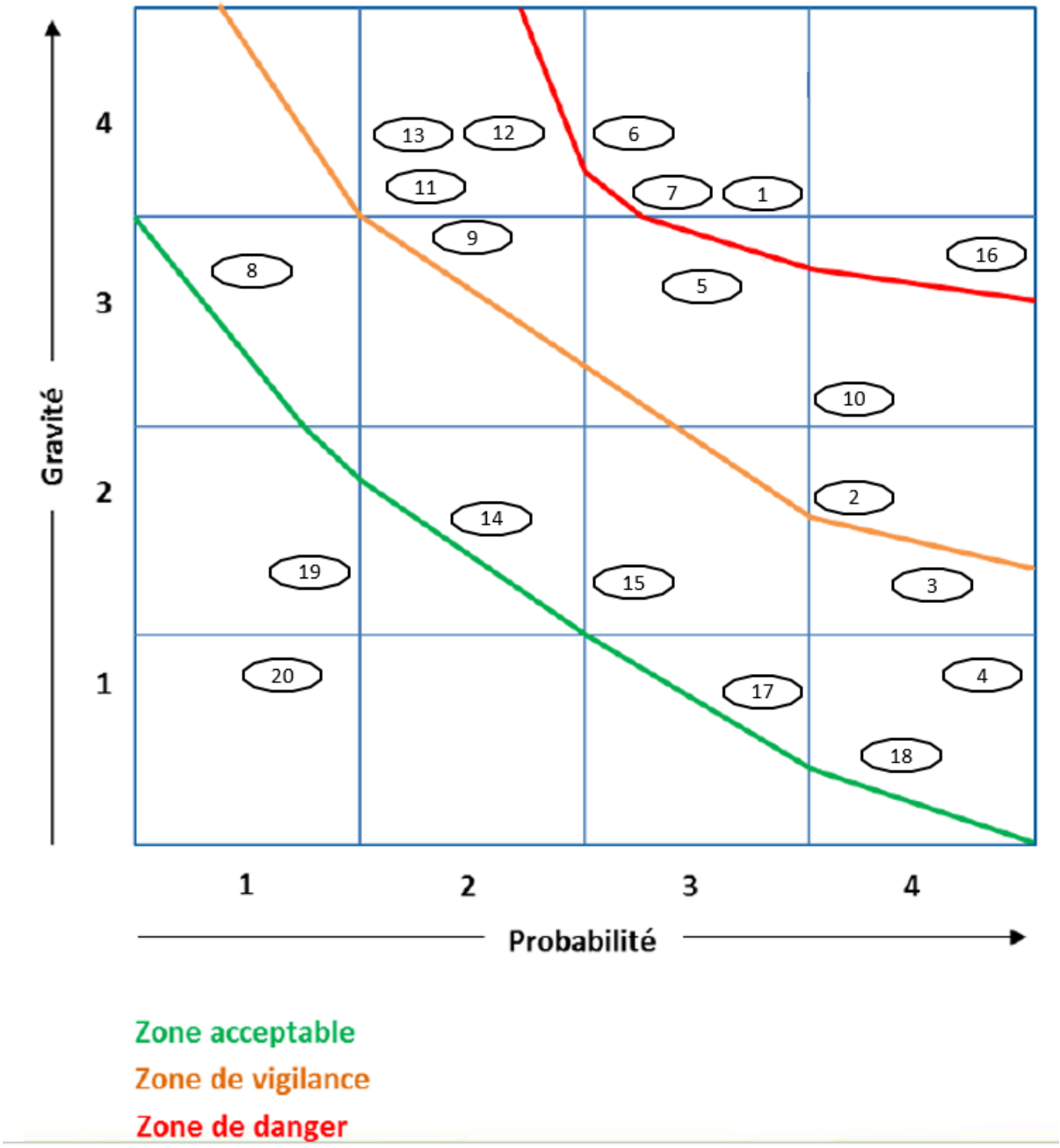


Comme vu précédemment, pour bien situer le positionnement du risque terroriste à travers l'ensemble des risques de sûreté, il est primordial de réaliser une cartographie des risques. Elle est techniquement dénommée « cartographie de l'aléa ». Pour le domaine de la Sécurité/Sûreté, elle est plus communément appelée « Cartographie des risques sécuritaires » en entreprise par abus de langage. En effet, elle comprend aussi les risques de sûreté. Cet outil va varier d'une entreprise à une autre. Cela dépend de son domaine d'activité, de sa taille, de son positionnement géographique. En soi, cela dépend de son exposition au risque d'une part, mais aussi de l'appréciation que fait le Risk Manager de cette exposition au risque.

La cartographie ci-après correspond à une analyse des risques de sûreté uniquement pour l'entité Nestlé France. Elle constitue un travail d'échanges et de recherches auprès des équipes de Nestlé en France, des usines et des clients. L'avantage de la cartographie des risques est qu'elle offre une représentation graphique et visuelle des risques.

La hiérarchisation est réalisée selon des critères de natures différentes. C'est une classification qui va aider le Risk Manager à prioriser ses actions de prévention et de protection au quotidien. Il va ainsi détecter quels risques doivent être assurés en priorité. Mais aussi, il va pouvoir orienter sa communication en fonction des enjeux relevés.

Dresser ce schéma n'est absolument pas une obligation. Certaines entreprises vont accorder plus ou moins d'intérêt à cet exercice. En revanche, la cartographie n'est jamais un processus « neutre ». L'entreprise qui réalise une cartographie des risques prend conscience de ces derniers. Ainsi, si le risque se réalise, et que l'entreprise savait qu'il était probable que l'événement se produise, alors elle peut être considérée comme responsable. Les collaborateurs, mais aussi les tiers, qui ont connu un préjudice peuvent effectuer un recours contre l'entreprise si cette dernière était consciente du risque mais n'a pas agi, ou n'a pas pris les mesures nécessaires.



Cartographie des risques de sûreté d'un groupe agroalimentaire

L'exemple de Nestlé France

Réalisation : Pauline Stevance, 2018

Légende de la cartographie

01	Incendie protestataire
02	Accident lors d'un événement
03	Malveillance, vandalisme, incivilité
04	Vol
05	Acte terroriste à l'encontre des marchandises et du matériel

06	Acte terroriste à l'encontre des personnes
07	Explosion
08	Prise d'otage
09	Pollution majeure
10	Colis, véhicule, bagage piégé

11	Véhicule suicide
12	Bombe humaine
13	Bombe radiologique
14	Violences urbaines
15	Violences physiques

16	Cybercriminalité
17	Délinquance
18	Fraude
19	Détournements d'actifs
20	Corruption

Le travail de cartographie ci-dessus a été réalisé par Pauline Stevance en collaboration avec M.Guillon, Directeur Sécurité/Sûreté de Nestlé France et M.Martin, Risk Manager de Nestlé France.

Ci-après, les risques mis en lumière par le travail de cartographie seront explicités plus en détail. Les choix de classification de ces risques reposent sur l'appréciation des équipes Risk Management et Sécurité/Sûreté de Nestlé France, sur l'expérience des Responsables de ces équipes et les spécificités du domaine de l'agroalimentaire.

Incendie protestataire : ce type d'incendie est un délit car il s'agit d'un incendie volontaire. Il est causé délibérément par l'Homme. La destruction volontaire des biens peut être faite avec ou sans la mise en danger d'autrui. Dès lors que la vie humaine est touchée, les conséquences sont toujours plus lourdes.

Dans le cas présent, pour l'entreprise Nestlé France, la fréquence et la probabilité sont élevées pour ce risque. Nestlé France dispose de nombreuses usines, de dépôts, de centres de stockage et distribution ainsi que de bureaux sur tout le territoire français.

Son exposition aux incendies volontaires ou plus précisément protestataires (c'est-à-dire lorsque les malfaiteurs visent l'entreprise ou le pays en particulier) est très forte. Beaucoup de collaborateurs travaillent dans les sites Nestlé, la vie humaine peut être facilement atteinte par l'incendie protestataire.

Ce risque peut potentiellement être exploité par des organisations terroristes, et de fait, il ne faut pas le négliger sur la cartographie ; bien qu'il puisse englober d'autres malfaiteurs que des terroristes. Fort heureusement, les matériaux utilisés aujourd'hui dans le domaine de la construction sont bien plus résistants au feu qu'auparavant.

La sécurité civile et l'intervention rapide des pompiers (chaque site doit se trouver dans une zone d'intervention basée à moins de dix minutes d'une brigade de pompiers) permettent de mieux appréhender le risque d'incendie protestataire bien qu'il reste l'un des risques les plus dangereux et inattendus.

Accident lors d'un événement : Nestlé France dispose détient des marques diverses et variées (Purina, Herta, Nescafé, Nestlé Waters, Nespresso, etc…). La société organise fréquemment des événements pour promouvoir ses produits. Ces événements peuvent être visés en raison de la notoriété de la marque. La couverture des risques liés à l'événementiel est particulièrement spécifique.

Il est possible d'assurer les accidents qui se produisent lors d'un événement mais la couverture et les garanties vont dépendre de la nature de l'événement concerné. Les mesures de prévention fixées en amont, la couverture assurantielle du risque ainsi que la gestion du risque en partenariat avec les départements Risk Management et Sécurité/Sûreté permettent de placer ce risque dans la zone de vigilance au sein de la cartographie.

La fréquence est relativement élevée mais la sévérité (*id est* : gravité) est plus faible. C'est davantage le risque d'image qui peut être lié au risque d'accident lors d'un événement. En revanche, si lors d'un événement organisé par Nestlé il y a un rassemblement de foule, les enjeux diffèrent et il faut mettre en place un dispositif sécurité/sûreté adapté. Pour chaque événement est réalisé un Risk Assessment (évaluation des risques) en amont.

Malveillance, vandalisme, incivilité : Les actes de malveillance, de vandalisme et les incivilités au sens large sont des cas rencontrés assez souvent par une entreprise comme Nestlé. La fréquence est donc élevée mais les impacts sur le « business » restent faibles.

Il y a ici une réelle volonté de nuire et de dégrader les biens de l'entreprise. Il peut s'agir par exemple de tags sur les murs d'une usine, de bris du matériel, etc…

Vol : le vol est un risque très fréquent, très probable pour une entreprise qui exerce dans le domaine de l'agroalimentaire. Vol de recettes, d'équipements, de matériels, de véhicules… Nestlé sait se prémunir de ce risque et dispose de couvertures assurantielles solides lorsque l'événement se produit.

Acte terroriste à l'encontre des marchandises et du matériel : il peut s'agir ici d'une attaque d'un train ou d'un camion transportant des marchandises identifiables (c'est-à-dire comportant le logo de Nestlé ou de la marque concernée) ou non identifiables (matières premières). Les conséquences financières peuvent être lourdes et la production peut être bloquée.

Les plans de continuité d'activité permettent de maintenir un niveau de production minimal durant la gestion du sinistre ou de disposer d'alternatives provisoires. Aussi, l'assurance va réduire les pertes financières accusées par le site. En revanche, l'atteinte à l'image de l'entreprise reste importante, surtout si les marchandises ou le matériel sont identifiables et mentionnent Nestlé.

Acte terroriste à l'encontre des personnes : cette catégorie est sans doute l'une des plus délicates à classifier. La probabilité (comme pour la catégorie précédente) est volontairement assez élevée sur la cartographie puisque l'exposition au risque n'est pas mesurable de manière précise.

Il convient de se baser sur des faits concrets : Nestlé est le leader mondial de l'agroalimentaire, son siège social français est basé en Ile de France et ses collaborateurs et expatriés voyagent à travers le monde entier.

Ces éléments permettent d'affirmer que Nestlé peut potentiellement être une cible pour de nombreux malfaiteurs y compris les organisations terroristes.

Cette catégorie est donc ici considérée comme la plus dangereuse puisqu'elle combine la réalisation de plusieurs risques : risque d'image, risque de décès/blessures des collaborateurs, risque matériel et perte d'exploitation.

Explosion : là encore, il s'agit d'un risque placé au niveau de la zone de danger. Le risque d'explosion en entreprise est assez bien maîtrisé aujourd'hui avec la classification des zones ATEX[8] et les audits de sécurité qui en découlent.

Mais lorsque l'explosion est réalisée volontairement par un individu, la maîtrise du risque est plus faible. Les conséquences sont désastreuses pour le site touché et la vie humaine.

Prise d'otage : ce type de risque concerne majoritairement les collaborateurs en déplacement ou les expatriés qui pourraient se trouver dans des zones à fort risque d'enlèvement ou de prise d'otages. Mais pas seulement : pour rappel, la prise d'otage par les frères Saïd et Chérif Kouachi le 9 janvier 2015 a eu lieu dans une imprimerie de Dammartin-en-Goële.

Ce site était protégé par un gardien et disposait d'un service d'alarme et de sécurité. Face à des forcenés détenant des armes telles que des Kalachnikov, un lance-roquettes et des cocktails Molotov, aucun dispositif ne pouvait résister.

La probabilité d'occurrence de ce risque reste malgré tout très faible selon les départements Sécurité/Sûreté et Risk Management de Nestlé France.

Pollution majeure : pour ce risque la probabilité est également faible mais la gravité est plus élevée puisque le seuil de vigilance est atteint. Le propre de l'agroalimentaire est de nourrir les populations.

Si une source d'eau de Nestlé Waters est contaminée ou bien si les matières premières présentes des corps étrangers, les conséquences peuvent être désastreuses au niveau sanitaire. Avec l'utilisation de détecteurs spécifiques comme les DPM (détecteurs de particules métalliques) ainsi que le suivi des équipes d'ingénierie, la détection de la pollution

[8] Zone ATEX : Atmosphères explosives. Explosions pouvant être créées par des poussières ou des poudres sur le lieu de travail. Règlementation ATEX issues de deux directives européennes ; 2014/34/UE et 1999/92/CE.

est réalisée rapidement aujourd'hui. La contamination délibérée de produits Nestlé pourrait avoir un impact très fort sur le sérieux de l'entreprise et la gestion de sa Supply Chain.

Colis, véhicule, bagage piégé : ce risque peut toucher tant les collaborateurs en déplacement que les sites Nestlé directement. Cette catégorie englobe donc des événements très divers et variés. Il peut s'agir de la réception d'un colis piégé contenant des explosifs par une usine ou un bureau de Nestlé. Ou encore, d'un bagage piégé volontairement échangé pour un collaborateur Nestlé en déplacement.

Au niveau du transport de marchandises, il est fréquent que des passagers clandestins soient retrouvés dans les remorques. La plupart du temps ce sont des migrants qui souhaitent rejoindre un autre pays clandestinement et ils sont souvent inoffensifs. Mais si des migrants, qui disposent de peu de moyens financiers, parviennent à rentrer dans la remorque d'un camion sans être aperçus, qu'arriverait-il si des terroristes utilisaient ce mode opératoire pour se déplacer ou piéger un véhicule ?

C'est en tenant compte de ce type de scénario que le Risk Management et la Sécurité/Sûreté de Nestlé France ont maintenu cette catégorie de risque dans la zone de vigilance.

Véhicule suicide : c'est un risque plutôt « nouveau » ou du moins, dont on parlait peu avant l'attentat de Nice en 2016 sur la promenade des anglais. Ce type d'attaque est réalisé à moindre coût par les terroristes et il est difficile d'identifier leur véhicule qui souvent, sont des véhicules volés.

La mise en place de plots en béton et de zone de sécurité depuis 2016 permet de réduire l'exposition au risque. Malgré cela, si le risque se produit la gravité reste très lourde.

Bombe humaine : les attentats des dernières années ont montré que les forcenés étaient désormais souvent équipés de gilets explosifs. L'installation de portiques de sécurité à l'entrée des sites de Nestlé France garantit une réduction du risque de bombe humaine.

Cependant les répercussions d'une bombe humaine en usine différent de celles pouvant être connues sur un site tertiaire. La gravité reste donc ici très importante puisqu'un individu armé est difficilement maîtrisable par des civils même si les dispositifs de sécurité sont parfaitement organisés.

Bombe radiologique : plus connue sont le nom de « bombe sale », la bombe radiologique est une bombe chimique ou biologique de nature toxique.

On entend par toxique nucléaire, radiologique, biologique ou chimique (NBRC). Jusqu'à aujourd'hui, aucun terroriste n'a réussi à se procurer des matériaux radioactifs et à créer une explosion.

Certains groupuscules rattachés à Al-Qaïda sont parvenus dans les années 2000 à créer des matériaux pour fabriquer des dispositifs de dispersion radiologique[9]. Mais tous ont été arrêtés. Le risque ici est donc maintenu en haute gravité mais la fréquence d'occurrence reste faible.

Violences urbaines : les violences urbaines peuvent prendre différentes formes. Le contexte politique en France en 2018 retrace de fortes tensions. Les manifestations et violences urbaines sont nombreuses (ZAD – Zones à défendre – à Notre dames des Landes où les affronts entre « zadistes » et forces de l'ordre ont été musclés ; les violences urbaines avec attaque au mortier à Champigny-sur-Marne en mai 2018, à moins de quinze kilomètres du siège social de Nestlé France ; les blocus de lycées et universités…).

Toutes ces situations ne sont pas amenées à dégénérer grâce à l'efficacité des forces de l'ordre et aux dispositifs de sûreté mis en place. L'exposition au risque de violences urbaines pour Nestlé France n'est pas particulièrement élevée que ce soit en termes de fréquence ou de gravité. Il ne faut cependant pas l'exclure de la cartographie, ce risque faisant partie intégrante des risques de sûreté envisageables en 2018.

Violences physiques : ce risque reprend les violences pouvant être commises non pas à l'encontre des locaux de l'entreprise ou de ses équipements mais à l'encontre des collaborateurs. Les collaborateurs de Nestlé France sont nombreux (12.000 salariés sur tout le territoire français), sans compter les collaborateurs expatriés (plusieurs milliers). La probabilité de réalisation de ce risque est donc plus élevée que pour le risque de violences urbaines.

[9] Dispositif de dispersion radiologique ou DDR, est une autre appellation de la bombe radiologique.

Cybercriminalité : Le risque cyber est considéré comme le risque le plus probable pour l'année 2018. En 2017, l'attaque « WannaCry » a impacté de nombreuses grandes entreprises dont Nestlé France.

La sécurité des systèmes d'informations est renforcée et des équipes sont dédiées à la protection des données chez Nestlé. Malgré cela, la menace est réelle et surtout très forte. Au XXIème siècle, la guerre se fait aussi virtuellement et les multinationales sont les premières entreprises touchées par la cybercriminalité.

Délinquance : le risque de délinquance est étroitement lié au risque de malveillance, de vandalisme, et d'incivilité. Il est important pour les équipes Sécurité/Sûreté de distinguer ce risque puisqu'il reflète de la criminalité d'ordre sociale.

La délinquance est souvent évoquée chez les jeunes adultes ou les adolescents. Facilement influençables, ces individus peuvent être facilement entraînés vers les organisations terroristes. Ce risque de délinquance est maîtrisable pour Nestlé France compte-tenu de son activité.

Fraude : la fraude représente le fait de falsifier ou de dissimuler des éléments. C'est un acte délibéré de tromperie. Le risque de fraude est assez élevé pour Nestlé France. En effet, son rayonnement au niveau international et le nombre colossal de partenariats qu'elle lie l'expose fortement à des cas de fraude.

Il peut s'agir de fraude dans les documents officiels, de tromperie de la part d'un fournisseur ou d'un client… Ce risque semble maîtrisé notamment par les équipes Qualité de Nestlé France.

Détournements d'actifs : Nestlé est une société cotée en bourse qui détient de puissants actionnaires. Le détournement d'actif est un risque de sûreté qui pourrait être assimilés à la fraude.

Il est pourtant spécifique car il est réalisé au détriment de l'entreprise mais au profit d'un tiers. Nestlé France reste peu exposée à ce risque mais son patrimoine pourrait être affecté par ce type de risque.

Corruption : la corruption est encore un autre risque causé par l'Homme. C'est un processus qui va être détourné pour masquer une activité frauduleuse.

Dans le cadre de la thématique traitée ici, le risque terroriste, la corruption tient une place particulière. En amont d'une attaque terroriste, il y a une réelle organisation et préparation.

Durant cette période, de nombreux facteurs entrent en jeu : qui fournit les armes aux terroristes ? Qui leur donnent des informations ? Qui les aident ? La corruption est considérée comme le « terreau du terrorisme »[10].

En effet, les organisations terroristes de Daesh et Boko Haram ont fait l'objet de financement par des gouvernements et des entreprises corrompus pour financer leur arsenal. Le risque de corruption est faible pour une entreprise de l'agroalimentaire.

Mais si un collaborateur de l'entreprise se radicalise et participe au financement du terrorisme, les conséquences pour l'image de Nestlé seraient désastreuses. Plusieurs entreprises ont été visées par les rapports de dénonciation de corruption et terrorisme. C'est le cas de Facebook et Google notamment.

2) Historique des différents attentats ayant impactés des entreprises

Dire que le terrorisme a toujours existé est chose aisée. Encore faut-il pouvoir l'expliquer et le justifier par des faits concrets. Comme vu précédemment, les premiers actes terroristes recensés en France sont ceux de la période de la Terreur de novembre 1793 à juillet 1794. C'était alors du terrorisme d'Etat.

C'est à partir du XIXème siècle que le risque terroriste individuel s'est développé. Deux premiers attentats échoués ont marqué l'histoire. Le 24 décembre 1800 pour l'attentat de la rue Saint-Nicaise et le 28 juillet 1835 pour l'attentat du boulevard du Temple à Paris. Ces actes terroristes visaient bien des « icônes » symbolisant la monarchie : l'empereur Napoléon Bonaparte et Louis-Philippe Ier.

[10] Article d'Enjeux les Echos par Brice Couturier, 9 mars 2015 : corruption et terrorisme.

Le bilan fut sombre pour ces deux attentats malgré leur échec : 22 morts, 28 blessés graves et une centaine d'autres blessés pour l'attentat contre Napoléon Bonaparte, ainsi que 46 logements détruits dans cette rue Saint-Nicaise (qui n'existe plus aujourd'hui à Paris). Et un total de 19 morts et 42 blessés dans l'attentat contre Louis-Philippe Ier.

L'intérêt de ce retraçage historique est tout d'abord de montrer que les modes opératoires utilisés pour les attaques terroristes n'ont pas tant évolué depuis le XIXème siècle.

Du moins, pour les attaques « physiques », les cyber-attaques d'aujourd'hui relevant d'une autre dimension.

Ce qui est flagrant c'est que le terrorisme individuel ciblait une icône, un personnage en particulier. Les civils n'étaient pas la cible directe, ils sont malheureusement des dommages collatéraux de ces deux attentats échoués. En l'occurrence, il s'agit de deux tentatives d'assassinat qui ont complétement été non maîtrisées par leurs auteurs respectifs.

Il n'était en soi pas prévu dans le plan d'attaque des terroristes de l'époque de blesser et de tuer des civils. Les monarques n'en auraient d'ailleurs eu que faire ; l'humain et la société civile n'étant pas au cœur de leurs préoccupations.

En 2018, la donne a complétement changé. Les civils sont devenus la cible directe pour semer le trouble et viser indirectement un personnage public, une institution, une entreprise ou un état. Le terrorisme religieux et dogmatique ainsi que le nouveau terrorisme individuel, connus depuis le XXème siècle, illustrent des actes de violence et de barbarie de plus en plus nombreux.

La première fois que la population a été prise pour cible directe d'une attaque terroriste était le 3 décembre 1947. Un train postal express de nuit alliant Paris à Tourcoing dans le Nord a déraillé, faisant 16 morts et plus de 30 blessés. Il s'agissait d'un sabotage réalisé dans le but de dénoncer les grèves des cheminots et des mineurs.

En effet, en 1947, au sortir de la seconde guerre mondiale, une grève nationale est tenue. Les cheminots et les mineurs s'opposent à la politique de rationnement mise en place par le Gouvernement alors en place.

Mais ce contexte de grèves crée de fervents conflits entre grévistes et non-grévistes. Ainsi, le sabotage réalisé est un acte, criminel, d'opposition à la SNCF et aux grèves de l'époque. Les auteurs de cet acte ne sont pas seulement des saboteurs puisqu'ils auraient très bien pu incendier un dépôt de la SNCF, détruire une zone de stockage ou même s'attaquer aux cheminots. L'action réalisée ici le premier acte de terrorisme au sens auquel il est entendu et appréhendé aujourd'hui.

Ce déroulé historique n'a pas vocation à être descriptif ou redondant. Il permettra au lecteur de mieux s'approprier les faits relatés ensuite.

a- Dans le secteur privé

Les entreprises du secteur privé ont souvent été prises pour cible lors d'attaques terroristes notamment en raison des symboles qu'elles véhiculent : richesse, puissance, liberté d'entreprendre, etc… Les organisations terroristes veulent faire passer des messages forts et violents en attaquant l'entreprise qui, par essence, est vouée à créer de la valeur et à réaliser des profits.

Attaquer une entreprise privée n'est pas similaire au fait d'attaquer l'Etat ou le Gouvernement du pays de manière directe. C'est une strate « intermédiaire » entre le fait de viser l'Etat lui-même ou de prendre la population pour cible. Lorsque les terroristes cherchent à atteindre l'entreprise, les civils sont nécessairement impactés.

Depuis le XXème siècle les attaques terroristes commises envers les entreprises du secteur privé en France sont de plus en plus nombreuses. Les premières entreprises directement touchées furent des journaux, des librairies. Là encore, le symbole est très fort puisque c'est l'une des libertés les plus chères aux citoyens français qui est visée : la liberté d'expression.

La liberté d'expression est reconnue en France depuis la Déclaration des Droits de l'Homme et du Citoyen de 1789. L'article 11 du texte indique que « la libre communication des pensées et des opinions est un des droits les plus précieux de l'homme ; tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi ».

L’attentat de janvier 2015 contre le journal Charlie Hebdo n’est donc pas une première. Une librairie maoïste fut explosée à Paris en 1968 par un parti d’extrême-droite, les journaux Le Parisien libéré, la Nation et Minute furent également attaqué en 1970 et 1971.

Mais avant ces tragiques événements, ce sont d’autres acteurs économiques proches des entreprises, les banques, qui ont été prises pour cible lors d’attentats terroristes. La première banque touchée fut l’Eurobank à Paris (la banque commerciale pour l’Europe) en 1951 puis la banque Worms, toujours située à Paris.

Ces deux attentats à l’explosif n’ont fait aucune victime. Plusieurs banques ont été fréquemment prises pour cible comme en décembre 1968 où trois banques furent attaquées dans Paris.

Tout au long du XXème siècle et depuis le début du XXIème, de nombreuses attaques terroristes ont été perpétrées envers de grandes entreprises et marques implantées en France. Les plus célèbres enseignes touchées sont : Chanel en 1981, les « Grands Magasins » (les Galeries Lafayette et le Printemps) en 1985, le centre commercial « Les Quatre Temps » de la Défense en 1986, le magasin Tati lors de l’attentat de la rue de Rennes en 1986, ou encore un restaurant McDonald’s en 2000.

Or, c’est en se concentrant sur les attaques terroristes plus récentes en France que les Risk Manager des entreprises peuvent tenir compte des risques psychosociaux qui en découlent. Gérer une menace en interne passe tout d’abord par la compréhension des émotions et des sentiments qui peuvent s’en dégager. Pour le risque terroriste, l’anxiété et le stress qui y sont liés sont particulièrement forts.

Le risque terroriste s’est amplifié en France depuis 2012. L’historique réalisé ci-après permet de contextualiser les événements.

11 et 19 mars 2012 - Toulouse et Montauban: Mohammed Merah tue 7 personnes.

7 janvier 2015 – Attentat de Charlie Hebdo: 17 victimes à Paris.

9 janvier 2015 - Prise d'otages à l'Hyper Cacher.

19 avril 2015 - L'attentat manqué de Sid Ahmed Ghlam.

26 juin 2015 - Un patron décapité à Saint-Quentin-Fallavier.

21 août 2015 - Attaque d'un Thalys empêchée par des militaires américains.

13 novembre 2015 – L'attentat le plus traumatique : le Bataclan d'autres attaques simultanées dans plusieurs bars et restaurants de la capitale, ainsi qu'aux abords du Stade de France. 413 victimes recensées.

13 juin 2016 - Deux policiers sont tués dans les Yvelines.

14 Juillet 2016 - Nice visée pendant son feu d'artifice par un camion-bélier. 87 victimes.

26 juillet 2016 - Le prêtre Hamel est assassiné à Saint-Etienne-du-Rouvray.

4 septembre 2016 - Des bombonnes de gaz sont découvertes à proximité de la cathédrale Notre-Dame.

3 février 2017 - Des militaires sont attaqués au Carrousel du Louvre.

18 mars 2017 - Une patrouille de Sentinelle est attaquée à l'aéroport Paris-Orly.

20 avril 2017 - Un policier est abattu sur les Champs-Élysées.

6 juin 2017 - Attaque au marteau à Notre-Dame de Paris.

19 juin 2017 - Une nouvelle attaque survient sur les Champs-Élysées.

9 août 2017 - Des militaires de l'opération Sentinelle sont attaqués à Levallois-Perret.

1er octobre 2017 - Attaque de deux jeunes femmes à l'arme blanche à la gare Saint-Charles de Marseille.

23 mars 2018 – Attaques simultanées à Carcassonne et dans un supermarché Super U à Trèbes.

12 mai 2018 – Attaque à l'arme blanche sur l'avenue de l'Opéra à Paris.

Lorsque la présente étude a été initiée, la plus grande crainte de l'auteure était que cette liste chronologique ne s'enrichisse davantage. Les premières attaques connues en ce début d'année 2018 et la fin de l'Etat d'urgence fin annoncé fin 2017 devaient être synonyme d'une accalmie mais la menace terroriste continue de peser sur la France.

Lors des rencontres de l'AMRAE à Marseille en février 2018, les assureurs et les Risk Managers ont décrit le risque terroriste comme l'une des menaces les plus fortes pour cette nouvelle année. Plus que jamais, le secteur privé doit se protéger et mettre en place des dispositifs de sûreté efficaces pour lutter contre le terrorisme.

b- Dans le secteur public

Le secteur public représente plus directement la Nation, l'Etat, le Gouvernement que les entreprises du secteur privé, qui y sont liées de manière intrinsèque. Les entreprises appartenant au secteur public sont beaucoup plus vulnérables et particulièrement exposées au risque d'attentat.

Au niveau historique, c'est au XXème siècle que commencent les attaques terroristes les plus sanglantes avec tout d'abord l'OAS, l'organisation armée secrète. C'est la première fois au cours de l'histoire française que des attaques terroristes sont réalisées en raison d'une décision de politique étrangère. En 1960, Le Gouvernement français souhaite quitter l'Algérie mais une organisation clandestine composée d'anciens militaires va s'y opposer, par tous les moyens.

Les attaques de l'OAS sont les plus connues de l'histoire du terrorisme en France. Leur bilan de 1961 à 1968 est en effet désastreux : 2.700 victimes sur les sols français et algérien. D'ailleurs, avant les événements de novembre 2015 en France, l'attaque terroriste la plus meurtrière en France remontait au 18 juin 1961 et avait été perpétrée par l'OAS.

Des membres de l'OAS avaient repris le mode opératoire utilisé lors de l'attaque du train postal express de 1947. Le sabotage des rails sur la ligne Strasbourg-Paris causa 170 blessés et 27 morts. Le XXème siècle fut le théâtre de nombreux massacres commis par l'OAS et par d'autres organisations terroristes, principalement dans des lieux publics ou dans les transports publics.

A travers les décennies, les transports en commun et les gares ont en effet connu des dizaines d'attentats. De nombreux voyageurs y transitent et les gares, bus et métro sont très faciles d'accès.

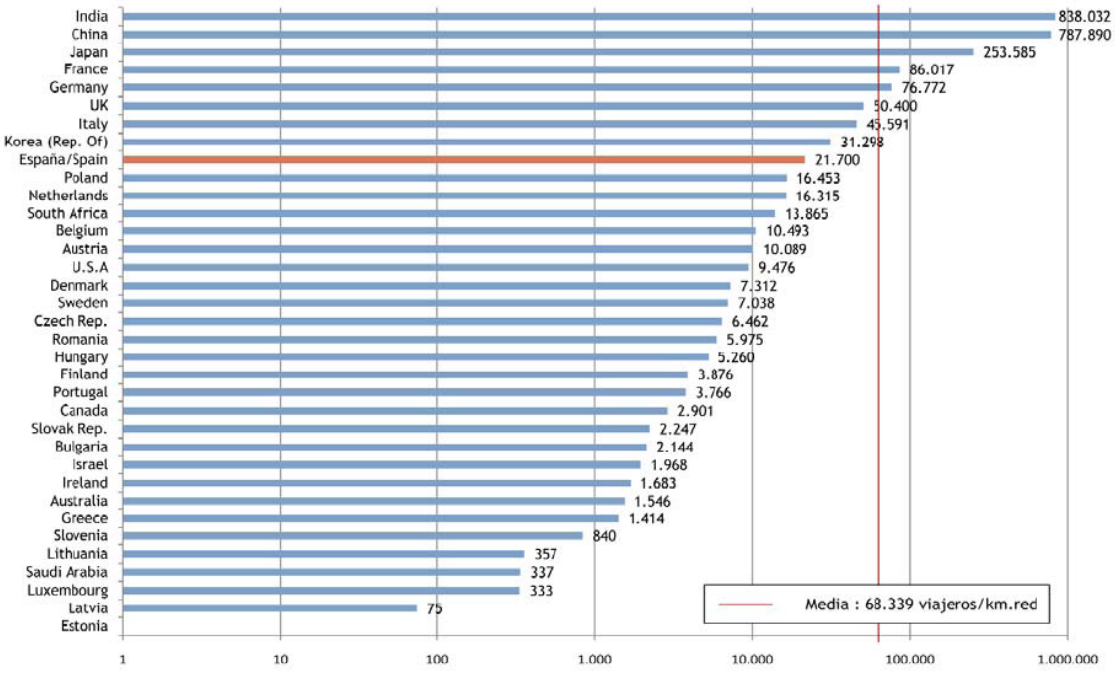
La sécurité et la sûreté des transports publics en France est fréquemment remise en question par le grand public du fait de cette accessibilité et du peu de contrôles réalisés. Le cas de la SNCF est assez représentatif de la menace terroriste dans les transports en commun.

Le réseau TGV en France représente un volume considérable de flux de voyageurs. Il y a plus de 3.000 gares en France, 6 millions de Français prennent le train chaque année et 15.000 trains circulent chaque jour. La sécurité et la sûreté mises en place au sein des réseaux ferroviaires d'autres pays sont considérées comme plus efficace par les médias français que celles appliquées en France.

C'est le cas de l'Espagne, ou d'Israël, qui sont souvent pris en exemple dans les médias français pour représenter l'efficacité des processus de sûreté et de sécurité à mener. En Espagne, tous les bagages sont passés au rayon X avant la montée des voyageurs dans les trains. Pour Israël, ces contrôles sont renforcés par des fouilles au corps.

A la différence près que les lignes espagnoles et israéliennes sont bien moins fréquentées que le réseau ferroviaire français. *De facto*, réaliser des contrôles de bagages, comme en Espagne, serait particulièrement coûteux et chronophage pour la SNCF, voire même irréalisable pour les effectifs présents en gare.

Le schéma ci-après représente, à titre indicatif, le nombre de voyageurs utilisant le réseau ferré par kilomètre de voie à travers le monde. Source : ICU, Janvier 2014.



B] LA GESTION ACTUELLE DU RISQUE TERRORISTE

1) Parallèle des solutions adoptées dans le secteur public et le secteur privé

a. Dans le secteur privé

Avec le retraçage historique réalisé précédemment, les entreprises privées apparaissent comme des cibles nouvelles. La coopération entre les entreprises du secteur privé et les entreprises du secteur public est inéluctable aujourd'hui tant la menace est forte et imprévisible. Les entreprises du secteur privé sont exposées aujourd'hui à un terrorisme « d'opportunité » notamment en raison du fait qu'il est plus simple pour une organisation terroriste de réaliser une attaque dans un magasin ou un restaurant plutôt qu'à l'Elysée.

Depuis le début du XXIème siècle, nous faisons face à un changement de cibles passant d'acteurs représentatifs du pouvoir à des acteurs représentatifs de la société. Le partage des bonnes pratiques et de connaissances en termes d'appréhension et de gestion du risque terroriste a permis, surtout au cours des attaques subies en 2015 en France, de faire face à une menace à laquelle aucun acteur n'avait alors songé.

C'est la réunion de différents acteurs économiques qui a permis d'éviter que les attentats connus ne se transforment en actes d'« hyperterrorisme ». L'hyperterrorisme a été dénommé la première fois après les attentats du World Trade Center le 11 septembre 2001. Cette expression est donc utilisée en cas de destructions et massacres à grande échelle, comme ce fut le cas aux Etats-Unis en 2001.

Lire le bilan de cette catastrophe humaine donne encore des frissons, même dix-sept ans plus tard : 2.977 morts, des milliers de blessés, des centaines de personnes jamais retrouvées ou identifiées, 200 unités de pompiers mobilisées sur les lieux.

Les actes terroristes connus en France relèvent du « terrorisme de masse » et non de l'hyperterrorisme. L'attaque qui détient le bilan le plus sombre à ce jour est celle du Bataclan, le 13 novembre 2015. Le bilan de cette fusillade de masse est de 137 morts et 413 blessés.

La salle de spectacle n'était en l'occurrence absolument pas prête à affronter ce type d'attaque.

Les forces de l'ordre et les secours ont d'ailleurs été également « surpris » puisque plusieurs attentats se déroulaient simultanément dans Paris. Or, dans cette immense tragédie connue par les français, il y a malgré tout une forme de « chance » : le fait que l'attaque du Bataclan ne se soit pas déroulée au Stade de France.

La France n'a pour le moment pas été confrontée à l'hyperterrorisme et des difficultés de gestion du risque ont déjà été identifiées face au terrorisme de masse. Donc, comment les entreprises du secteur privé peuvent-elles se protéger au maximum contre le risque terroriste ? Quels investissements faut-il réaliser et sur quelles stratégies faut-il miser ?

En ce qui concerne les commerces et la distribution, ces domaines sont désormais vulnérables et sensibles face au risque terroriste. La situation est assez différente dans les commerces de proximité par rapport aux grandes surfaces.

La menace terroriste y est jugée moins élevée. Mais aucune structure ne peut s'estimer épargnée aujourd'hui, quelle que soit sa dimension, son secteur d'activité ou sa zone géographique. Les attaques ont en effet une plus grande probabilité de se produire dans des centres commerciaux ou des grandes surfaces – comme cela a déjà été le cas dans de nombreux pays – car les terroristes se donnent pour objectif de tuer le plus de monde possible, de faire le plus de victimes.

Mais depuis la prise d'otages du magasin Hyper-Cacher en janvier 2015 à Paris, le terrorisme de proximité s'est fortement développé. Dans les semaines qui suivirent les attentats de novembre 2015, les commerces ont d'ailleurs connu une forte baisse de fréquentation.

Sécuriser leur activité est devenu un véritable challenge pour conserver leurs clients. Le chiffre d'affaires réalisé par les grands magasins avait chuté de 25% début décembre 2015 et d'un peu moins de 20% pour les centres commerciaux. Il y a donc bien évidemment un enjeu humain et sécuritaire, mais aussi un enjeu financier derrière cette prévention du risque terroriste. Les enseignes de distribution ont bien saisi l'intérêt de miser sur la sécurité.

C'est le cas des centres commerciaux Auchan, qui ont mis en place un plan de formation interne pour les salariés, sur des thématiques de sécurité et de sûreté.

Pour d'autres distributeurs c'est la surveillance humaine qui a été au cœur des plus gros investissements. D'ailleurs, la surveillance par agents a augmenté de 15%[11] dans la distribution en 2015. Au total, la surveillance humaine a représenté des dépenses à hauteur de 410 millions d'euros à fin 2015.

Ces chiffres peuvent sembler démesurés mais l'investissement sur la surveillance humaine a permis aux distributeurs et aux commerces de réduire dans le même temps leur exposition face au risque de vol. Ceci a contrebalancé, en partie, les investissements réalisés.

Avant 2015, le secteur de la sécurité privée était plutôt en régression. Mais avec les attentats de 2015, la sécurité privée a connu un véritable rebond. En effet, les investissements réalisés en termes de sécurité par les commerces et la distribution comprennent non seulement la surveillance humaine mais aussi la sécurité électronique, la sécurité physique, les procédés de lutte anti-incendie, etc…

Selon une étude réalisée en 2016 par *En Toute Sécurité* (journal spécialisé dans les questions de sécurité et sûreté*)*, les dépenses de sécurité ont atteint 1,3 milliard d'euros en 2015 et continuent de progresser encore aujourd'hui.

Ces investissements sont réalisés majoritairement par les grandes enseignes, mais les petits commerces s'équipent de plus en plus de matériels et d'outils pour renforcer leur sécurité et leur sûreté à leur échelle. Il s'agit d'équipements de télésurveillance ou d'alarmes essentiellement mais aussi de systèmes de contrôle d'accès. Ceci n'assureraient pas la protection absolue des commerces en cas d'attaque, mais permettraient d'identifier un assaillant ou, pour les autorités, de maîtriser davantage le risque.

Le secteur privé a un rôle bien plus grand à jouer auprès des français dans la lutte antiterroriste. Que ce soit au niveau de la sécurité des salariés ou des clients, chaque entreprise peut à son échelle agir contre le risque terroriste et participer à cette lutte, pour la Nation.

[11] Source : Perifem, association technique des enseignes de grande distribution, des commerces spécialisés et des centres commerciaux.

b. Dans le secteur public

La partie précédente, qui reprend les dates clefs du terrorisme en France, démontre que les entreprises du secteur public sont historiquement plus exposées à la menace terroriste. Ce sont des entreprises, des collectivités locales ou encore des administrations publiques qui représentent directement l'Etat français.

Pour les entreprises du secteur publique, l'Etat détient *a minima* 51% de leur capital social. L'Etat peut donc « exercer directement ou indirectement une influence dominante du fait de la propriété, de la participation financière ou des règles qui régissent »[12] cette entreprise.

Cette influence de l'Etat se ressent dans la culture et la mise en œuvre de procédés dans ces entreprises publiques. Aussi, les modes de gestion et de traitement du risque, dont le risque terroriste, sont différents de ceux rencontrés dans les entreprises du secteur privé.

Après les attentats connus en France au cours des dernières années, l'Etat a demandé aux citoyens de faire preuve de résilience. Les représentants de l'Etat ont souhaité que les français gardent avant toute chose leur attachement à leurs valeurs républicaines et démocratiques.

Mais comment les français, de nouveau mis à l'épreuve avec l'attentat de Nice le 14 juillet 2016, peuvent-ils être résilients alors que l'ensemble de la société n'était pas unis ? En effet, les pouvoirs de l'Etat ont rapidement été remis en question dans l'opinion publique en termes de sécurité et de sûreté. L'Etat, et donc les entreprises du secteur public, sont les garants de la sécurité sur le territoire. En cas d'attaque, c'est bien vers eux que les citoyens se tournent.

Focus sur la perception du risque terroriste dans trois grandes entreprises du secteur public – dont l'Etat est actionnaire majoritaire – et les collectivités territoriales.

EDF pour « Électricité de France » est le premier producteur et fournisseur d'électricité en France mais aussi en Europe. L'Etat français dispose de 83,5% de cette entreprise. Comme détaillé en partie 2) a, l'activité d'EDF est spécifique puisqu'elle touche au nucléaire.

[12] Définition donnée par les textes de l'Union européenne – article 2 de la Directive 80/723/CEE de la Commission du 25 juin 1980 relative à la transparence des relations financières entre les États membres et les entreprises publiques

Face à la menace terroriste, l'entreprise dispose d'un arsenal de processus intégrés et de plans de continuité solides (car testés régulièrement). EDF a aussi une campagne de communication interne redoutable.

Les salariés sont conscients du risque et ne le craignent pas. Ils sont formés pour pouvoir garder leur calme et appliquer les protocoles en vigueur lorsque la menace se réalise. Tout semble expliquer la raison pour laquelle EDF n'est que très peu exposée au risque terroriste.

L'accès à ses usines nucléaires est extraordinairement difficile. Aussi, dès que l'Etat français module la réglementation relative aux sites industriels, EDF est le premier lieu d'intégration de ces mesures. L'entreprise publique, qui plus est, à « hauts risques », se doit d'être un modèle pour l'ensemble des acteurs de l'industrie française.

La Française des Jeux a été créée en 1976. C'est une entreprise publique dont l'Etat possède 72% des parts. L'entreprise détient le monopole sur les jeux de loterie, les jeux à gratter et les paris sportifs en France.

Compte-tenu des réformes économiques menées actuellement, l'Etat français compte revendre ses parts de la Française des Jeux en 2019. Mais en attendant, l'entreprise relève toujours du service public.

Quel lien la loterie nationale peut-elle avoir avec le risque terroriste ? Sans surprise : le blanchiment d'argent et le financement du terrorisme. Le 8 mars 2017, un trafic de blanchiment d'argent a été démantelé par les forces de police à Aulnay-Sous-Bois.

Ce blanchiment se faisait par le biais de rachat de tickets de la Française des jeux. Les forces de l'ordre ne savent aujourd'hui pas exactement à quelles fins cet argent a été utilisé. La somme était pourtant colossale puisque le trafic était en place depuis plus de deux ans. Au total, plus d'un million d'euro aurait été blanchi.

La Française des Jeux est tenue à une obligation de vigilance à l'instar des banques. Elle signale chaque année plus de 10 millions d'euros liés à d'opérations suspectées frauduleuses aux autorités dont « Tracfin[13] ». Il s'agit d'un organisme du ministère de l'Économie et des Finances, chargé de la lutte contre le blanchiment d'argent et le financement du terrorisme.

[13] Tracfin signifie : traitement du renseignement et action contre les circuits financiers clandestins.

Les nombreux points de vente qui commercialisent les fameux tickets de loterie ne sont pas tous vertueux. Argent et terrorisme sont intrinsèquement lié par le blanchiment, mais pas que. La Française des Jeux dispose de très nombreuses données.

Comme vu précédemment, la Data est le nouvel or noir. La Française des Jeux dispose d'un Data Protection Officer, en charge de la protection des données. En effet, l'entreprise détient une masse d'informations précieuses : noms et coordonnées des gagnants, adresses et informations relatives aux banques, transactions réalisées, etc…

Elle a donc mis en place un partenariat avec IBM pour pouvoir utiliser le Big Data. C'est grâce au criblage de données que la Française des jeux peut désormais détecter efficacement les comportements suspects.

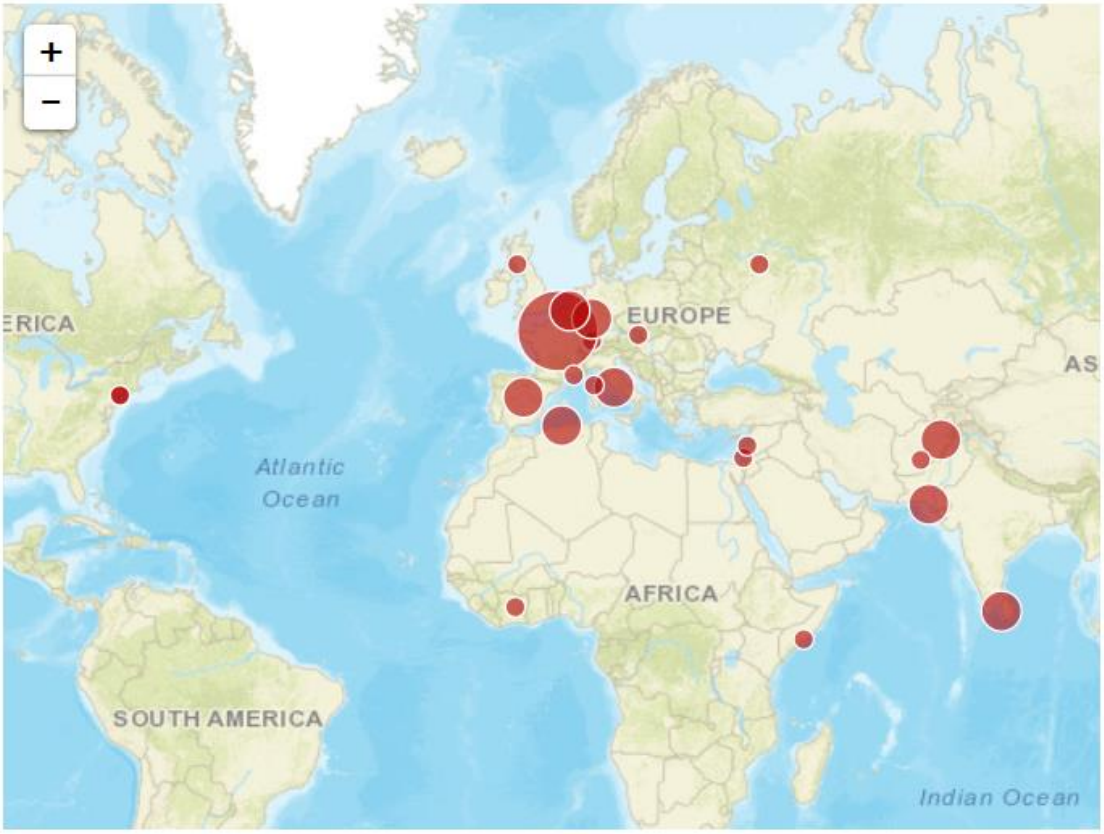
Les Aéroports de Paris sont aujourd'hui détenus à haut de 50,6% par l'Etat. Ce cas est un peu plus spécifique, puisqu'en mars 2018 le gouvernement a indiqué qu'il souhaitait vendre la totalité de ses parts d'ici la fin de l'année.

En attendant, les aéroports de Paris dits ADP, restent une entreprise du secteur public à l'heure de la présente étude. Le domaine des transports est vulnérable face à la menace terroriste. Les attentats du World Trade Center ont profondément marqué ce secteur d'activité.

Mais ce ne sont plus tant les avions qui sont les cibles privilégies des organisations terroristes mais bien les aéroports eux-mêmes. Les attentats dans les aéroports de Bruxelles et Istanbul (triple attentat suicide) en 2016, Karachi en 2014 ou encore Moscou et Francfort en 2011 ne sont qu'une infime partie du nombre d'attentats perpétrés dans les zones aéroportuaires.

Ainsi, au cours des cinquante dernières années trente-quatre attaques terroristes ont été commises dans des aéroports à travers le monde[14], dont des fusillades, des attaques à la bombe ou encore des opérations commando. La carte ci-dessous illustre le fait que la plupart des attaques ont eu lieu en Europe. L'aéroport d'Orly, au sud de Paris, a d'ailleurs été touché quatre fois par ce type d'attaque.

[14] Source : M. De l'Espinay, journaliste pour le Parisien.



Source : journal le Parisien, numéro du 22 mars 2016.

Les aéroports restent donc des « soft target », des cibles dont la vulnérabilité est très élevée malgré le renforcement des politiques de sûreté effectué au cours des dernières années. D'autres « soft target » comme les transports en commun (bus, trains ou métros), les hôpitaux, les écoles, les centres commerciaux ou les restaurants ont un point commun : leur accessibilité.

Dans tous ces lieux, des dégâts mortels à grande échelle peuvent être commis. Restreindre les accès de ces lieux au maximum sous-entend le fait de mobiliser des ressources budgétaires colossales. Mais ne serait-ce pas le moyen le plus efficient pour mettre un terme à ces attaques ?

Ces dernières sont très coûteuses, au niveau humain tout d'abord mais aussi sur le plan économique. Renforcer la sécurité en réduisant l'accessibilité des zones aéroportuaires est sans nul doute le meilleur investissement à réaliser.

A titre d'exemple, dans les aéroports israéliens, c'est plus d'onze contrôles qui sont réalisés avant l'embarquement des passagers. Ces contrôles viennent en plus de la surveillance par les forces de l'ordre (patrouilles d'agents en civil). L'Etat d'Israël est le pays qui dispose des meilleurs résultats en termes de sûreté et de sécurité face à la menace terroriste puisque le gouvernement et la population sont particulièrement attachés aux mesures de prévention.

En France, les aéroports étaient davantage sécurisés il y a plusieurs décennies mais comme l'indique Alain Bauer[15] « nous sommes passés d'une époque où les aéroports étaient difficiles d'accès, à une logique de tourisme de masse, d'interconnexion, d'ouverture sur la ville et d'effacement des frontières. Revenir en arrière sera très compliqué ».

Les collectivités territoriales ou collectivités locales (dans le langage courant) sont des personnes morales rattachées à l'Etat. Elles différent en ce sens des entreprises. Elles disposent cependant d'une certaine autonomie et restent bien distinctes de l'Etat lui-même. Il s'agit des communes, des départements et des régions mais il existe aussi des collectivités territoriales spéciales comme la ville de Paris.

Ces acteurs ne sont pas directement touchés par le risque terroriste mais ont un rôle prédominant à jouer en termes de prévention et de sûreté. Les actions des pouvoirs publics vont être souvent d'ordre répressif notamment sur le plan militaire. Alors qu'au niveau des collectivités territoriales, un travail à long terme est réalisé pour prévenir le risque et surtout pour lutter contre la radicalisation.

Certaines collectivités territoriales ont commencé en 2015 à mettre en place des programmes de sensibilisation à la menace terroriste dès l'école primaire. Le fait de pouvoir mettre des mots sur ce que les enfants perçoivent dans les médias est, selon les collectivités territoriales, un moyen d'éviter l'endoctrinement chez les jeunes.

Certaines idéologies comme le djihadisme entendu selon Daesh, ciblent les jeunes qui s'estiment oubliés ou persécutés par la France et ses institutions. Les jeunes en grande difficulté scolaire et ceux qui commettent des actes de délinquance sont les plus visés par les organisations terroristes.

[15] Alain Bauer est professeur de criminologie appliquée au Conservatoire national des arts et métiers et consultant en sécurité français.

La posture adoptée par les collectivités territoriales va plus loin encore, puisque certains maires ont mis en place des programmes d'accompagnement psychosociaux pour les individus radicalisés afin de tenter de les réinsérer dans le système classique.

Ces démarches ne peuvent bien entendu pas être appliquées au monde de l'entreprise compte tenu des enjeux économiques. L'Etat, et donc les collectivités territoriales se doivent d'assurer une sûreté publique. Les entreprises doivent se concentrer sur la sûreté afférée à leur périmètre.

En revanche, il était important de détailler ces démarches établies par les collectivités territoriales ici puisque les entreprises pourraient s'en inspirer. Le travail réalisé par les mairies et les régions est un travail de long terme. Ce n'est pas aux entreprises de mettre en place des programmes de réinsertion des radicalisés (mais après tout pourquoi pas ? Si cela permet d'annihiler le risque ?), mais c'est bien à elles que revient le rôle de « défenseur privé ».

De facto, s'inspirer des actions menées par les collectivités locales est plus qu'intéressant pour deux raisons : elles allouent des ressources budgétaires conséquentes à la prévention du risque et déploient leurs actions à long terme.

En effet, en 2017, ce ne sont pas moins de 65 millions d'euros qui ont été alloués au plan d'action national des collectivités territoriales contre la radicalisation et le terrorisme. Ce plan d'action comporte la sécurisation des écoles (23 millions d'euros), le programme de réinsertion et de citoyenneté (20,7 millions d'euros) ou encore la sécurisation des sites sensibles ou espaces publics (5,8 millions d'euros).

Parallèlement, la prévention de la délinquance a représenté 34 millions d'euros d'investissement cette même année[16].

[16] Source : chiffres issus du journal « MaireInfo », à destination des maires et des élus locaux.

2) Les lacunes des modes de gestion d'aujourd'hui

a. La complexification du risque : cyber attaques et industries à hauts risques

Le nombre d'attaques cybercriminelles contre les entreprises ne cessent d'augmenter. Le fait de savoir que des réseaux mortifères, tels que ceux des organisations terroristes, peuvent pirater des systèmes d'informations précieux aux entreprises n'est pas particulièrement rassurant pour les Risk Manager.

Les cyberattaques ne doivent en aucun cas être négligées. Au cours des semaines qui ont suivi l'attentat du journal "Charlie Hebdo", ce sont près de de 25.000 sites internet français qui ont été la cible de hackers islamistes[17]. Ces attaques ont, pour la plupart, consisté à remplacer la page d'accueil des sites par des messages incitant à la haine et faisant l'apologie du terrorisme.

Pour des entreprises, ces attaques sont particulièrement mauvaises pour l'image et la représentation des valeurs de l'entreprise. Mais les attaques les plus graves sont les atteintes et les piratages des systèmes d'informations. Si les réseaux de distribution en électricité sont piratés, les réseaux téléphoniques, ou encore la signalisation routière, nul ne peut dire quels seraient les dommages possibles.

Pour affronter cette menace, le recrutement de nouveaux métiers et profils est essentiel. Ils seront très importants pour la vie de l'entreprise de demain et pourront être particulièrement utile face aux cyberattaques. C'est le cas des Data Analyst, Data Owner, Data Scientist, Data Miner et Data Protection Officer. Ces experts de la donnée, la data, sont au cœur des réseaux et pourront détecter la menace terroriste plus rapidement et surtout la contrer.

La menace de cyberattaque est ciblée, opportuniste et diffuse. En effet, elle se propage sous forme de virus. Mais la nature des attaques ne cesse d'évoluer. Ainsi, les cyberattaques contre Sony en 2014 ou encore TV5 Monde en 2015 avaient pour but uniquement de détruire les réseaux.

[17] Information communiquée par Frédéric Valette, chef de la division cybersécurité à la Direction générale de l'armement (DGA).

Les hackers prennent le temps d'apprendre de leurs échecs et reviennent ensuite plus forts. C'est là que la menace s'accroît et se renforce. D'où la nécessité d'avoir des services et des collaborateurs spécialisés sur ce sujet.

La mutualisation des informations entre les acteurs économiques est, il faut le rappeler, essentiel pour pouvoir lutter contre le terrorisme. Les entreprises qui subissent des cyberattaques doivent déposer plainte. La police judiciaire étant tenue au devoir de réserve, le risque d'image ou d'atteinte à l'e-réputation est nul.

La majorité des entreprises ne s'inspirent pas suffisamment des processus intégrés dans les entreprises dites « NBRC » (nucléaire, radiologique, biologique ou chimique) pour lutter contre le terrorisme et mettre en place des actions de prévention et de protection du risque efficaces. Pourtant, c'est au sein de ces entreprises dites à « hauts risques » que la probabilité d'occurrence d'un événement de type terroriste est la plus faible.

Qu'il s'agisse du nucléaire ou de la pétrochimie, la présence de substances toxiques dans ces entreprises sous-entend la nécessité de politiques de prévention et de protection solides. L'accès à ces entreprises est particulièrement difficile mais ce n'est pas la seule raison qui justifie une exposition faible au risque terroriste.

En effet, les matières nucléaires sont parfois amenées à être déplacées, ce qui aggrave donc la probabilité d'occurrence du risque terroriste. Si un camion est chargé de plutonium ou d'uranium, les conséquences pourraient être très lourdes en cas d'attaque. Cependant les transports de matières nucléaires sont très sécurisés en France. Ils se déroulent pour des raisons évidentes, de manière confidentielle afin de d'optimiser le niveau de sécurité au maximum.

Les dispositifs appliqués vont être adaptés selon le type matière transporté. S'agissant du transport de plutonium ou d'autres déchets radioactifs, il s'agit des mesures de sécurité et de sûreté les plus hautes. Les transports sont assurés par des camions, des trains ou des avions particuliers. Les forces de l'ordre garantissent un périmètre de sécurité lors des transports routier en suivant les convois sous forme d'escorte. Les responsables des opérations sont en contact permanent avec les autorités.

Les risques effectifs des centrales nucléaires en France sont surtout des risques environnementaux et sanitaires[18]. La menace terroriste est sous un contrôle quasi-absolu.

Dans le cas d'EDF, les actes de terrorisme ont été pris en compte dès l'ouverture des centrales nucléaires. Tout a été pensé, dans chaque projet de centrale, pour éviter ce risque. Plusieurs niveaux de protection sont mis en place afin de concentrer le risque dans une zone plus restreinte, ce qui en permet une meilleure maîtrise.

Des portiques de sécurité et des caméras de surveillance sont placés à chaque entrée. Ces dispositions sont aujourd'hui courantes dans les différentes usines françaises, quel que soit le secteur d'activité concerné. Mais à l'ouverture des premières centrales nucléaires – dès 1962 en France – ces restrictions d'accès et ces dispositifs étaient comparés à ceux des prisons ou centres pénitenciers.

Pourtant, ils ont démontré leur efficacité au fur et à mesure des années et ont été mis en place dans des domaines complétement différents. En Annexe 6 se trouve l'illustration de la protection d'une usine EDF.

b. L'imprévisibilité du risque : faille d'anticipation dans les procédés de gestion actuels

Le risque terroriste est un élément extérieur, exogène, à l'entreprise. L'entreprise dispose de peu de moyens en réalité pour agir sur ce risque. La clef pour maîtriser ce risque est la prévention. On parle de maîtrise du risque mais il s'agit plutôt de contention de ce risque et surtout d'en réduire les conséquences au maximum.

Les attentats terroristes qui ont frappé la France en 2015 ont clairement montré que le risque pouvait survenir partout, à n'importe quel moment ou période de l'année. Personne n'est à l'abri de la menace. Les attentats ont toujours existé mais c'est, depuis 2015, la forme de ces derniers qui a changé. La France a été prise pour cible et les messages des terroristes étaient extrêmement précis à l'encontre des pouvoirs politiques et du gouvernement français.

[18] Source : IRSN, Institut National de Radioprotection et de Sûreté nucléaire, information communiquée en janvier 2018.

Il ne faut tout de même pas omettre que ces messages politiques n'ont aucune légitimité à être considérés puisqu'ils proviennent de réseaux et groupuscules faisant partie de la grande criminalité. La France, en Etat de choc a donné trop d'importance à ces réseaux, ce qui les a malheureusement renforcés.

En sur-réaction, le gouvernement français a affirmé dans les médias que la France était en « guerre contre le terrorisme »[19]. Au-delà de la forme rhétorique le mot guerre enclenche tout un système juridique et institutionnel. C'est un renversement de tout ce qui est ancré dans les garanties du risque terroriste notamment au niveau assurantiel. Certaines polices d'assurance comportent des exclusions pour les situations de guerre. La tenue de tels propos, relayés par les médias, a fait désordre au sein des compagnies d'assurance et dans les services Risk Management des entreprises. En effet, en cas de guerre, certains risques ne peuvent plus êtes couverts par les compagnies d'assurance qui émanent du domaine privé ; en cas de guerre ces risques sont du ressort de l'Etat.

Le risque étant imprévisible, aucune faille dans la communication ne peut être tolérée, et les retours d'expérience ont montré que l'annonce non-officielle de « contexte de guerre » a semé beaucoup d'inquiétude inutilement. Ce dont il faut davantage se soucier en revanche, ce sont les « cellules dormantes ». Les cellules dormantes sont des individus qui ne sont pas encore passés à l'action. Et c'est bien là que faille d'anticipation dans les procédés de gestion actuels sont perceptibles.

La plupart des réseaux qui orchestrent le djihadisme et toute autre forme de terrorisme actuel, ont des « agents » présents sur le territoire qu'ils projettent d'attaquer. Ces individus ont été formés et entraînés en Afghanistan, en Tchétchénie ou en Lybie notamment.

Pour les entreprises françaises médiatiques et audiovisuelles, les messages relayés au public sont cruciaux. Les terroristes considèrent la société Occidentale comme « dépravée et corrompue »[20].

[19] Propos tenus par plusieurs politiques en 2015 suite aux attentats de Charlie Hebdo : Manuel Valls, Bernard Cazeneuve et François Hollande.
[20] Description de la société occidentale tenue dans une vidéo de propagande – transmission publique lors des rencontres de l'AMRAE à Marseille – Février 2018.

Lorsque les entreprises de presse prennent position ou décrivent le terrorisme de manière extrapolée, cela donne davantage de crédibilité aux organisations terroristes qui ne restent avant tout que des groupuscules. Plusieurs entreprises de presse ont découvert de façon simultanée avec le grand public la nouvelle menace terroriste en 2015.

Suite à l'attaque de Charlie Hebdo, ces entreprises sont devenues des cibles directes et elles ont dû renforcer leur politique de sécurité et de sûreté. Tout cela a été réalisé à très court terme, ne laissant pas de délai suffisant aux entreprises d'appréhender ce risque. Il a fallu qu'elles s'adaptent rapidement à affronter des agresseurs d'un nouveau genre et une forme de risque nouvelle.

Une autre faille de la gestion du risque terroriste en entreprise est la gestion de l'émotion et de la panique. Dans les premiers moments qui ont suivi les cellules de crise mises en place après les attentats de 2015 dans les entreprises, ce qui ressort est une courbe exponentielle d'émotion chez les salariés.

Le responsable de la Sécurité/Sûreté d'une entreprise de presse disait à ce sujet : « je me devais de rester calme. Mon obligation de résultat me force avant tout à protéger et rassurer les salariés en prenant les mesures nécessaires face à une situation de danger grave imminent »[21].

La charge émotionnelle qui pèse sur les Risk Manager et les Responsables de la Sécurité/Sûreté est conséquente. Mais le fait de parvenir à garder son sang-froid permet de déployer dans les meilleures conditions possibles les dispositifs d'urgence comme les cellules de crise ou les plans de continuité d'activité.

La relégation d'informations est devenue un élément essentiel dans ce nouvel univers des risques. Le terrorisme 2.0 sera sur la guerre de l'information. En effet, auparavant, le risque se basait sur l'obtention de la connaissance par autrui.

Or, une organisation terroriste comme Daesh a parfaitement assimilé le sens et l'ampleur de la détention d'informations. Daesh a créé des espaces informationnels indépendants et a

[21] Responsable Sécurité/Sûreté d'une grande entreprise de presse française – identité restée confidentielle puisque la menace terroriste pèse toujours très lourdement sur les entreprises de presse en 2018.

fortement utilisé les réseaux sociaux à savoir Facebook, Twitter et Youtube pour faire passer ses messages. Créé en 2006, Daesh est une sorte de « branche » de ses prédécesseurs d'Al-Qaïda. Cette organisation terroriste combat les forces qui s'opposent à l'islamisme radical en Syrie ainsi qu'en Irak.

L'enjeu pour faire face à ce genre d'organisation qui dispose de moyens et de savoirs colossaux n'est plus seulement de prendre de l'information mais aussi d'en fournir. Cela permet de déstabiliser les terroristes en utilisant des méthodes stratégiques telles que la rumeur, la diffamation ou encore la désinformation.

Dans les rangs de Daesh, il n'y a pas que de jeunes délinquants sous emprise qui n'ont pas beaucoup étudié ou qui ont peu de compétences spécifiques. Il y a aussi des ingénieurs, des médecins, des informaticiens… Daesh a su s'entourer très rapidement de professionnels de tous les secteurs pour pouvoir se déployer et imposer leur propagande et leur barbarie. L'organisation dispose d'ailleurs d'un « chargé de communication » du nom de Rafiq Abu-Moussab. Son activité consiste à gérer la présence de Daesh sur le web et à travers toutes les formes de médias.

Daesh a aussi dans ses rangs un informaticien du nom d'Ahmad Abousamra. Ce dernier est d'ailleurs diplômé de l'Université du Massachusetts aux Etats-Unis. Pire encore, Daesh a développé et structuré ses activités de propagande en créant des entreprises de presse et de production. C'est le cas des sociétés Al-Hayat ou Al-Itissam. La communication et la détention d'information représente la puissance de frappe de Daesh en Irak et en Syrie, et surtout partout à travers le monde.

Cette tendance à la guerre de l'information est inquiétante puisque cela représente des risques diffus, de moins en moins mesurables. Tous les groupuscules existants sont amenés à évoluer et à se complexifier.

A l'issue des attentats de 2015 en France, il est alarmant de constater que les services de renseignement français ne détenaient pas les ressources nécessaires pour faire face à ces forcenés. Le nombre d'unités à déployer, tant au niveau quantitatif que qualitatif – c'est-à-dire avec une formation et une expérience du terrain minimales – n'était pas suffisant.

En amont, les ressources économiques nécessaires à la surveillance de ces individus n'étaient que trop faibles. Ce n'est plus un seul individu qu'il faut mettre sur surveillance mais des centaines, comme c'est le cas avec le fameux fichier des fichés S où ils sont plus de 1000 à être enregistrés.

Dans le cas d'une attaque hyperterroriste, des dizaines de forcenés attaqueraient simultanément une ou plusieurs cibles. Les terroristes bénéficieraient d'une large préparation et auraient des timings fixés, tout serait préparé encore plus minutieusement, dans une clandestinité absolue des échanges et des communications. Le temps est le facteur le plus important dans la gestion du risque terroriste. C'est l'unique facteur sur lequel les entreprises peuvent jouer en cas d'attaques multiples et/ou simultanées.

A la lumière des différents attentats qui ont eu lieu au cours des dernières années, il est clair que toute entreprise peut être visée par un acte terroriste. La première étape de prévention est d'intégrer ce contexte puis d'être en mesure d'évaluer la capacité de résistance et de réaction de l'entreprise face à une situation de crise.

Partie 2 : La recherche de nouvelles méthodes pour gérer le risque terroriste.

A] DES PROCEDES NOVATEURS

1) A la source du risque : les nouveaux protocoles de détection et d'identification du risque terroriste en entreprise

a. L'intérêt des retours d'expérience

Les retours d'expérience, plus communément appelés « REX » dans le jargon des entreprises, sont la clef de la dernière étape de la mission du Risk Manager. Les retours d'expérience représentent la pièce maîtresse du suivi et du contrôle des risques. Ci-après, la schématisation des grandes étapes de la gestion du risque terroriste.

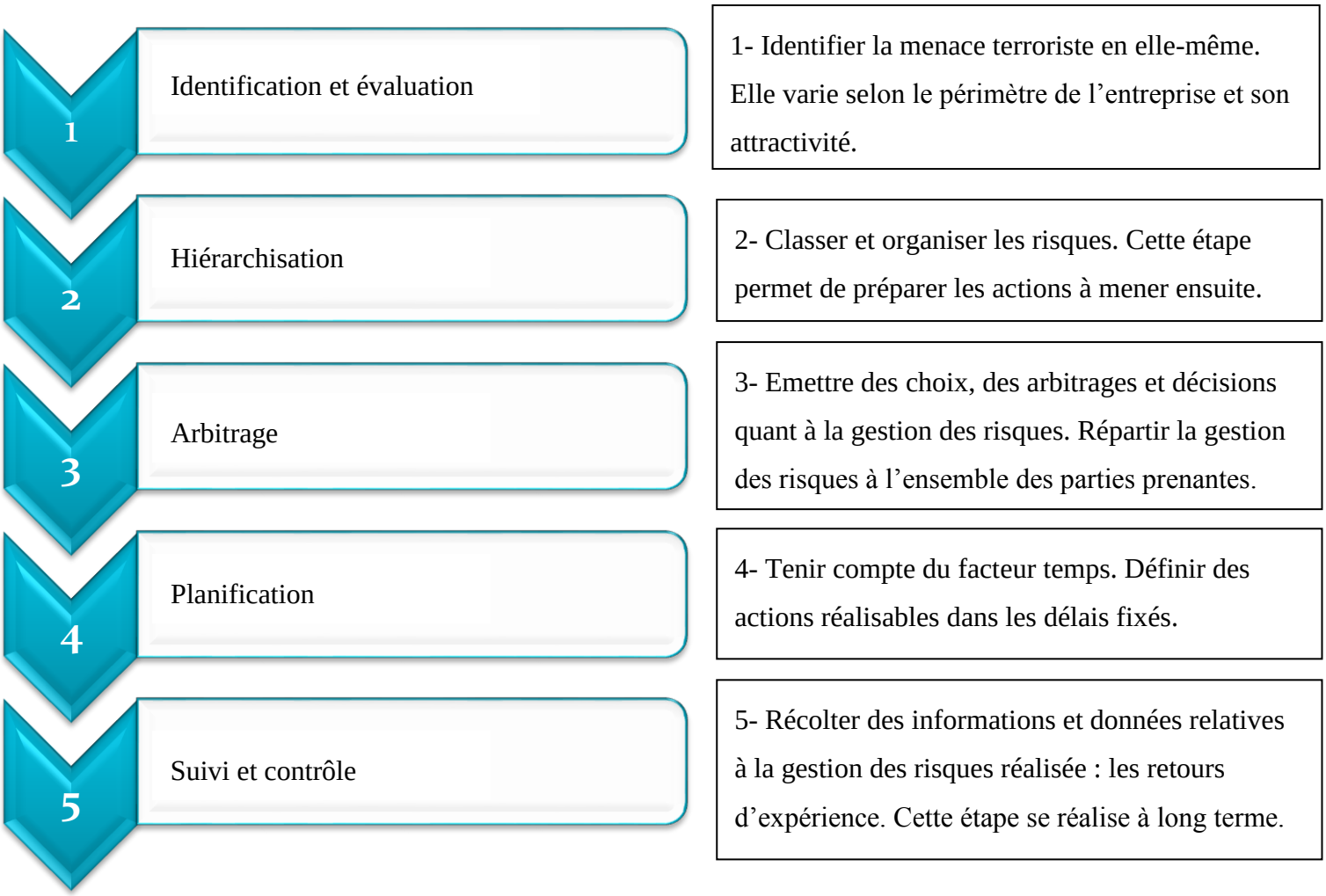


Schéma : les étapes clefs du Risk Management appliqué au risque terroriste

Pauline Stevance, 2018

Les retours d'expérience sont obtenus à la fin du processus de gestion des risques. Or, ils permettent ensuite de mener une identification et évaluation des risques (étape 1) plus efficace. Ce processus est donc cyclique. Un bon traitement des retours d'expérience, le fait de communiquer autour de cela et surtout de les suivre de près, va améliorer la gestion des risques.

Par exemple, si un individu dangereux s'est introduit dans un bâtiment ou dans un magasin d'une entreprise, les retours d'expérience vont permettre d'identifier les failles dans les mesures de sécurité appliquées.

Ainsi, un audit de sécurité peut-être mené afin de renforcer la protection des sites de l'entreprise, quels qu'ils soient. Les retours d'expérience et l'étape de suivi et contrôle dans sa globalité font partie d'une démarche d'intégration de la sécurité en amont. Pour gérer et traiter un risque majeur, il faut se questionner sur ce dernier avant son apparition.

Dans le cas des attentats du World Trade Center aux Etats-Unis en 2001, il était particulièrement difficile d'identifier ce type risque : personne n'avait imaginé qu'un avion pouvait être détourné pour heurter les tours jumelles. Le Risk Manager, comme « chef d'orchestre » des acteurs de la sécurité et de la sûreté en entreprise, va mettre en place, suite à ces retours d'expérience, des Risk Assessments[22]. Ces Risk Assessments sont souvent réalisés en petit comité, uniquement avec les acteurs qui connaissent le risque ou le projet concerné.

Ce genre d'exercice fait appel à la réflexion des différents services de l'entreprise (SHE[23], Service Qualité, Risk Management, Sécurité/Sûreté, Ingénierie, etc…). La mise en commun des connaissances et compétences de chacun est une force. Réaliser le Risk Assessment du risque terroriste de l'entreprise en amont permet d'être prêt et conscient du risque lorsque l'événement se produit.

Grâce au travail de suivi et contrôle, une stratégie de sécurité multimodale peut être développée au sein de l'entreprise. De quoi s'agit-il ? C'est la mise en place de dispositifs intégrés sur l'ensemble des sites de l'entreprise.

Il s'agit de la surveillance humaine par le biais des agents de sécurité, l'installation systématique de portiques et de caméras de vidéosurveillance à chaque entrée. Aussi, pour protéger les accès et réduire le risque d'intrusion au maximum les systèmes d'alarmes sont essentiels et il est primordial de prévoir des équipements technologiques adaptés à cette menace terroriste qui se modernise sur tous les champs (drones, outil de reconnaissance faciale, etc.). Dans la stratégie multimodale de l'entreprise sont également intégrés les outils annexes dont les PCA, plans de continuité d'activité.

[22] Risk Assessment : atelier d'échanges, de cartographie et de discussions autour d'un risque spécifique ou d'un projet en cours.
[23] SHE : service sécurité, hygiène et environnement.

Aussi, l'auto-assurance n'est plus une option aujourd'hui dans le cadre du risque terroriste. L'ensemble des grandes entreprises l'ont bien compris et elles disposent en majorité de polices d'assurance gérées par des courtiers internationaux ou des assureurs de renommées mondiales. Le cas échéant, lorsque l'entreprise souhaite gérer elle-même son risque, ce sont des captives d'assurance qui sont créées et gérées par les entreprises elles-mêmes.

Néanmoins, la couverture du risque terroriste est réalisée de manière assez satisfaisante par le domaine de l'assurance. Il existe de nombreuses solutions sur le marché et des couvertures qui regroupent les risques politiques, ce qui permet aux entreprises de bénéficier de polices complètes pour leurs risques de sûreté.

Il y a en revanche des difficultés qui sont exprimées, notamment si lors de l'attaque terroriste commise, il n'y a aucun dommage matériel. Au niveau assurantiel, cela pose des problématiques quant à l'indemnisation des entreprises assurées.

Aussi, des coûts additionnels parfois conséquents peuvent être réclamés à l'assureur. Ce sont des surcoûts nécessaires à la poursuite d'activité notamment quand les entreprises concernées ne peuvent relancer la production pour des raisons de sûreté.

Les retours d'expérience ont aussi permis d'identifier des lacunes dans la gestion de l'information en situation de crise. L'amplification du terrorisme a conduit à un sentiment d'insécurité générale : les citoyens se sont sentis visés tout comme les entreprises. En effet, le profil du terroriste est vaste et il est possible de le rencontrer dans la rue ou sur son lieu de travail. Une forme de paranoïa a été ressentie après chaque attaque terroriste en France.

Il est désormais nécessaire que toutes les entreprises utilisent le criblage numérique pour détecter le moindre signal de radicalisation émanant de la part de ses salariés. Ceci va permettre de solidifier toutes les investigations réalisées par les forces de l'ordre et les services de renseignement dans la gestion des données et de l'information. Mais aussi, la mutualisation des informations entre pouvoirs publics, assureurs, courtiers et prestataires doit être optimisée.

b. L'évolution des procédures de détection (pour les tiers et pour les salariés de l'entreprise)

Le risque terroriste affecte tant les tiers (clients, fournisseurs) que les salariés de l'entreprise. Au niveau humain, les processus de détection passent tout d'abord par la qualité de la cible du risque : est-ce que des voyageurs sont visés ? Des expatriés ? Des locaux ? Ou encore, des sous-traitants ?

Toutes ces cibles peuvent être présentes, parfois simultanément, lors d'un attentat. Elles peuvent être sujettes à un enlèvement ou bien se trouver dans des zones affectées par le terrorisme. Pour agir, l'entreprise doit passer par une première étape de gestion du risque : identifier et évaluer toutes les phases du risque – cf. schéma en page 46 schématisation des grandes étapes de la gestion du risque terroriste.

Le sujet de la radicalisation en entreprise s'avère particulièrement délicat. Il est souvent évoqué à demi-mot, comme tabou. Obtenir des informations sur cette problématique est plus que laborieux. La radicalisation d'un collaborateur rappelle que les terroristes, malgré leurs actes monstrueux, sont des êtres humains et qu'ils peuvent être partout. Ils peuvent avoir une vie de famille, un emploi, et être intégrés en entreprise, avant de commettre du jour au lendemain, l'irréparable.

L'un des responsables de la Direction Générale de la Sécurité Intérieure précise[24] que la radicalisation en entreprise ne peut être traitée par une fonction à elle seule. Le Risk Manager et le Directeur Sécurité/Sûreté ne peuvent œuvrés de manière indépendante sur ce sujet. Il faut non seulement que toutes les fonctions soient conscientes de cette problématique et qu'elles l'appréhendent selon leur angle de vue, mais aussi, il faut que toutes les fonctions interagissent ensemble sur la radicalisation en entreprise et s'échangent des données. Cela relève essentiellement des ressources humaines.

Au 1er janvier 2017 aux Aéroports de Paris, évoqués précédemment, le Préfet a déposé 87 refus ou retraits d'habilitations des collaborateurs, pour des cas de suspicions de radicalisation religieuse.

[24] Entretien avec un des responsables de la DGSI, Direction Générale de la Sécurité Intérieure lors des rencontres de l'AMRAE en février 2018. Pour des raisons de confidentialité, le nom de cet interlocuteur ne peut être précisé.

La radicalisation ne se fait en effet pas que dans les centres pénitentiaires ou les prisons. L'entreprise est devenue l'un des lieux de radicalisation les plus courants. Les organisations terroristes, bien qu'elles détiennent une certaine notoriété à travers le monde, sont sans cesse à la recherche de nouveaux individus pour rejoindre leur rang puisqu'elles restent avant tout des groupuscules.

Ainsi, un tiers des femmes terroristes aujourd'hui dans le monde n'avaient d'appartenance à aucune religion et sont des « converties » à l'islam radical. Du côté des hommes, les « convertis » représentent un quart des terroristes. C'est ainsi que la première femme terroriste arrivée sur les terres de Daesh était une belge flamande[25].

La vérification de l'identité de tous les nouveaux collaborateurs va permettre, en termes de prévention, de détenir un premier gage de sécurité. La demande de l'extrait de casier judiciaire B.3 (bulletin numéro 3 relatant les condamnations les plus graves) au collaborateur est un élément clef du recrutement. Mais aujourd'hui la vérification de l'identité du candidat passe aussi par des recherches sur internet et les réseaux sociaux pour les recruteurs.

De précieuses informations peuvent y être trouvées en complément des premiers renseignements obtenus. Cela apporte surtout une première idée de qui est le futur collaborateur de la société. Or, pour traiter de risque terroriste, il faut aller plus loin. Sur les différents sites de l'entreprise, des contrôles d'identité doivent être réalisés successivement. Le port de badges facilite la reconnaissance des individus (titulaires, stagiaires, intérimaires, fournisseurs…) et sécurise les entrées et sorties.

Au sein de Nestlé France, les tours de cou pour les badges sont de couleurs différentes en fonction du statut de chaque collaborateur. Le violet est la couleur utilisée pour les personnes extérieures au site, ce qui est particulièrement visible aux caméras pour les équipes sécurité/sûreté et le gardien. Le port du badge autour du cou, de manière visible est obligatoire au sein d'une entreprise comme Nestlé France. C'est le cas dans de nombreuses autres entreprises. Les personnes extérieures ne sont pas libres de se déplacer seules et doivent toujours être accompagnées.

[25] Source : site Internet stop-djihadisme.gouv.fr

Mais ces dispositions sont-elles suffisantes ? L'idéal serait en effet de pouvoir traiter les problématiques liées aux entrées et sorties des personnes extérieures en amont. Quoi de tel qu'un système de pré-inscription sur le site internet de l'entreprise des visiteurs ; avec enregistrement de leur document d'identité ?

Cette solution pourrait être mise en œuvre pour laisser le temps au service de sécurité/sûreté de vérifier l'identité des individus projetant de se rendre sur le site de l'entreprise avec si nécessaire la possibilité d'échanger avec les forces de l'ordre si besoin.

Le temps est un allié précieux dans la gestion du risque terroriste. Ce facteur doit être parfaitement intégré par toutes les équipes devant œuvrer dans la gestion et la prévention du risque terroriste en entreprise.

2) Les évolutions dans la gestion de ce risque : fonctions, compétences et dispositifs intégrés

a. La formation des salariés

La communication et la formation sont sans nul doute les moyens les plus efficaces pour les collaborateurs d'appréhender le risque terroriste. Dans des situations à hauts risques, chaque geste ou action peut altérer la résolution d'un problème. Depuis les attentats de 2015 en France, un véritable « élan citoyen » s'est fait ressentir.

C'est suite aux faits marquants de l'attaque du Bataclan qu'un réel engouement pour l'engagement civique s'est fait ressentir notamment autour des questions de sécurité et de sûreté. Beaucoup de débats ont eu lieu, sur la déchéance de nationalité ou encore le suivi des individus « fichés S » mais ce qui ressort fondamentalement du grand public et surtout des jeunes à l'issue des attentats de 2015 est cette envie de protéger autrui.

En 2016, les candidatures à l'armée ont explosées, de même pour la réserve opérationnelle et la Police nationale. Les inscriptions au service civique se sont aussi multipliées durant l'année 2016. Sans compter le nombre exceptionnels de candidats au concours des gardiens de la paix la même année : 30.000 candidats pour 2.000 places, du jamais vu.

Du côté des sapeurs-pompiers, le constat fut le même avec 6.000 individus inscrits aux sessions de sensibilisation au secourisme et à la protection civile.[26] La Croix Rouge a décrit cet élan citoyen comme une phase de résilience des français face au risque terroriste. Pour l'intégralité des acteurs de la prévention et de la gestion des risques il s'agit là d'une opportunité. Il y a un réel désir de formation dont il faut profiter pour que la culture du risque se transmette.

La formation des collaborateurs se déclinent sous plusieurs strates : les salariés affectés à la sécurité, les collaborateurs qui peuvent être exposés directement au risque (collaborateurs présents sur « le terrain » et en contact direct avec les clients ou collaborateurs fréquemment en déplacement) et enfin les collaborateurs potentiellement moins exposés.

En ce qui concerne les salariés affectés aux différents services en lien avec la sécurité/sûreté, les formations au risque terroriste vont être plus pointues. Pour les gardiens et veilleurs en usine ou sur site, on parle de gardiennage classique. Les formations de ces collaborateurs sont primordiales puisqu'ils ne détiennent pas d'arme et doivent adopter les bons comportements pour protéger l'entreprise et surtout se protéger eux-mêmes.

Il est aussi possible de faire appel à des agents de sécurité privée qui, sous certaines conditions et s'ils possèdent la formation adéquate, pourront utiliser des armes non létales (matraques de type bâton de défense ou tonfa[27], lacrymogènes etc.). Ou encore, il est possible de faire appel à des agents de sécurité privée pouvant être dotés d'une arme de poing.

Ces mesures sont en application depuis le 1er janvier 2018 (traduction réglementaire de loi du 28 février 2017 relative à la sécurité publique).

Les collaborateurs pouvant être directement exposés au risque sont les salariés en déplacement et ceux qui travaillent au contact de la clientèle. Ce sont deux éléments d'aggravation du risque terroriste en entreprise pour les salariés. Après les salariés affectés aux missions de Sécurité/Sûreté, ces collaborateurs doivent être formés en priorité au risque terroriste et aux bons gestes, aux bons comportements à adopter.

[26] Chiffres issus du rapport de M.Brandet, ministère de l'intérieur – 2017.
[27] Tonfa : type de matraque utilisée par les forces de l'ordre.

Enfin, tous les autres salariés de l'entreprise doivent *a minima* être sensibilisés au risque terroriste. Cela peut passer par des communications internes (campagne d'e-mailing, affiches, distribution de flyers) ou des ateliers thématiques avec inscription sur la base du volontariat. Dans les plus grandes entreprises, des conférences sont organisées et chaque collaborateur est libre d'y assisté ou non.

Ces démarches peuvent être onéreuses mais le gain réalisé en cas d'attaque terroriste peut être particulièrement élevé. Des individus informés de la posture à tenir, disposant des bons gestes pourront se mettre en sécurité plus aisément et surtout rester calme. Une personne *lambda*, qui n'a entendu parler du risque terroriste qu'à travers les médias ou Internet va davantage adopter un comportement de panique et pourra entraîner avec lui d'autres collaborateurs jusqu'à créer un potentiel mouvement de foule.

Au sein de Nestlé France, dans le cadre de la politique voyage, un partenariat est mis en place avec International Sos. Il s'agit de l'entreprise spécialiste du risque voyage et des flux de personnes à travers le monde qui édite notamment chaque année le célèbre Travel Risk Map (Annexe 2).

Nestlé a donc tissé un partenariat pour les collaborateurs puissent bénéficier d'un suivi personnalisé lors de leurs déplacements. Ainsi, si un collaborateur est amené à voyager, avant de prendre le départ, il doit appeler International Sos via une ligne téléphonique dédiée. Il reçoit des informations clés pour son déplacement : risque météorologique, menace terroriste, risque épidémiologique, etc…

Le schéma ci-après illustre ce procédé d'informations pré-voyage. L'illustration est en anglais pour qu'elle soit comprise de tous les collaborateurs. En effet, beaucoup de collaborateurs au sein de Nestlé France ne sont pas français et sont issus d'autres filiales de Nestlé dans le monde.

Si le collaborateur n'a pas la possibilité d'appeler le centre d'assistance d'International Sos pour recevoir les instructions, le service Sécurité/Sûreté de Nestlé France a songé à la mise en place d'une application mobile polyvalente.

Ce projet d'application mobile a été lancé en 2014 et servait à l'origine simplement à communiquer des instructions de voyage selon les destinations enregistrées. Il a été amené à évoluer depuis, surtout en raison des attentats de 2015 en France et la hausse du risque terroriste dans le monde.

D'autres données sont désormais intégrées comme la géolocalisation du collaborateur, des rubriques conseils et des bonnes pratiques. Le département Risk Management a approuvé cette démarche numérique. Mais en termes de continuité d'activité, cet outil d'application mobile n'était pas suffisamment fiable. En effet, selon les zones de déplacement, il n'est pas toujours possible pour un collaborateur de recharger son téléphone.

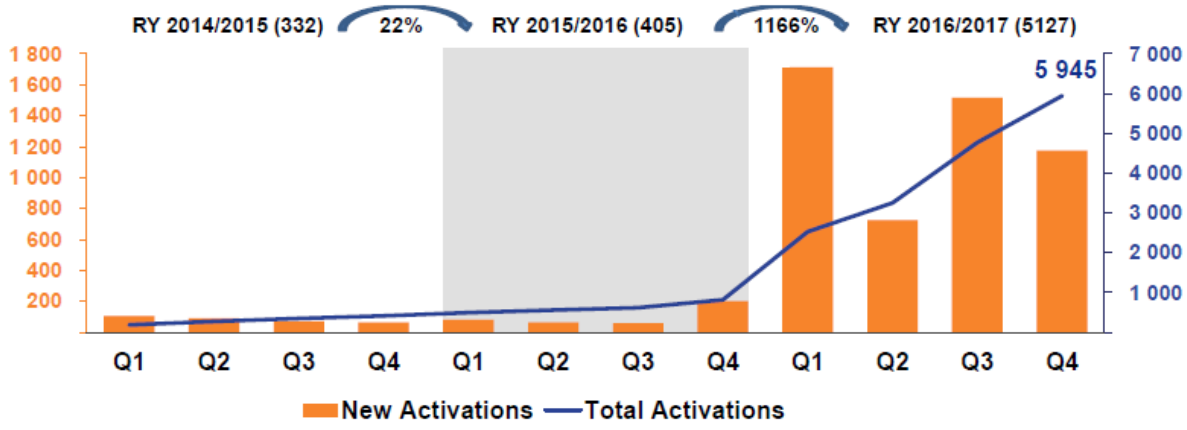
Afin de rester connecté en toutes circonstances à l'étranger ou en France, Nestlé France s'est associé à une entreprise, Ampy, qui propose de convertir l'énergie cinétique d'une personne

pour recharger son appareil mobile via une connexion USB. En marchant, l'utilisateur permet d'alimenter une batterie d'appoint d'une capacité de 1000mAh[28].

Ainsi, former un collaborateur pour qu'il puisse se déplacer et agir en toute sécurité ne passe pas uniquement par des sessions de formation en salle ou la fourniture d'outils sans donner d'informations concernant leurs utilisations.

Pour que les salariés soient capables d'adopter les bons gestes en cas de menace terroriste, il faut les sensibiliser et les former en amont mais surtout les accompagner et tenir compte de leurs contraintes au quotidien. A défaut, tout le travail de formation réalisé ne sera d'aucune utilité.

En plus de cela, il faut énormément communiquer. Cela se fait par le biais de tout ce dont peut disposer le salarié : les réunions, les boîtes mail, l'Intranet, les SMS, etc… Ainsi, le déploiement de l'application mobile a pris du temps puisque les collaborateurs n'y trouvaient pas de réelle utilité. Le graphique ci-dessous montre le nombre d'installations de l'application mobile sur les smartphones des collaborateurs entre mars 2014 et février 2017.



En 2014, le peu d'intérêt des collaborateurs face à cette application est clairement schématisé. C'est après les attentats de 2015 en France que le nombre d'installations a explosé.

[28] Produits Ampy : www.getampy.com/ampy-move

En complément, si les Risk Manager ou les Directeurs Sécurité/Sûreté ont besoin de supports pour appuyer leur communication, des fiches techniques ont été élaborées par le Secrétariat Général à la Défense et à la Sécurité Nationale (SGDSN) en relation avec les différents ministères. Suite aux attentats du 13 novembre 2015, une campagne de sensibilisation a été lancée pour mieux préparer et protéger les citoyens face à la menace terroriste[29].

b. Les fonctions du Risk Management et de la Sécurité/Sûreté en entreprise

Souvent, dans les grandes entreprises, les fonctions relatives au Risk Management et à la Sécurité/Sûreté sont distinctes. En effet, même s'il s'agit de gestion des risques, les risques de sûreté et de sécurité requièrent des compétences spécifiques et une expérience significative en matière de protection des populations.

Mais, conjointement, les fonctions de Risk Manager et de Directeur Sécurité/Sûreté sont fortement liées puisqu'elles ont un objectif commun : protéger les collaborateurs et le cœur de l'entreprise : le « business ».

Le Directeur de la sûreté et de la sécurité est amené, au regard de ses missions, à interagir avec des acteurs qui diffèrent des clients ou des fournisseurs. Par exemple, il peut avoir à contacter les forces de l'ordre ou encore les services de renseignement. Connaître l'armée et/ou la police, savoir comment communiquer auprès de ces interlocuteurs phares est un atout pour le Directeur Sûreté/Sécurité. C'est pour cette raison que grand nombre de Responsables Sûreté/Sécurité sont issus de carrières policières ou sont d'anciens militaires. Le domaine des forces de l'ordre possède en effet son histoire, ses principes et ses règles.

Pour mettre en place une communication optimale avec ces acteurs ainsi que des plans d'actions efficaces, il faut être en mesure de les comprendre et de savoir comment ils opèrent, quels sont leurs enjeux, quelle est leur culture, etc… De mauvaises relations avec les forces de l'ordre, les services de renseignement ou les représentants de l'Etat peuvent nuire fortement à la gestion du risque de sécurité et de sûreté en entreprise.

[29] Supports en ligne sur : http://www.gouvernement.fr/reagir-attaque-terroriste

Au niveau opérationnel, le Directeur de la sûreté et de la sécurité est en charge d'identifier les menaces mais aussi d'organiser et de mettre en œuvre la protection des personnes et des biens, la sensibilisation et la formation des personnels à la culture de sûreté, le support et le conseil technique.

L'aide à la gestion de crise constitue également un axe prioritaire de la mission Sûreté/Sécurité. Lorsque les départements Risk Management et Sûreté/Sécurité sont scindés, ces missions sont en effet bien distinctes.

Les spécificités principales du poste de Directeur Sûreté/Sécurité reposent sur sa capacité à intervenir sur les voyages et les déplacements au sens large des salariés et à réaliser un travail de veille. En lien avec les services informatiques et ressources humaines, il est possible pour le Directeur Sûreté/Sécurité de réaliser un « tracking des voyageurs ». C'est-à-dire, un suivi des déplacements professionnels (et personnels, en cas de déménagements ou d'expatriation par exemple). Dans les grandes entreprises, le Directeur Sûreté/Sécurité participe au développement de la politique voyage et de l'affrètement des moyens de transport.

Le travail de veille pour le Directeur Sûreté/Sécurité est axé, pour les années à venir, vers l'intelligence économique. Cela se lie transversalement à la gestion de la donnée, la Data.

Les terroristes 2.0 peuvent désormais s'attaquer aux bases de données des entreprises sans grande difficulté. Il convient donc de mettre un point d'honneur à la protection des systèmes d'information.

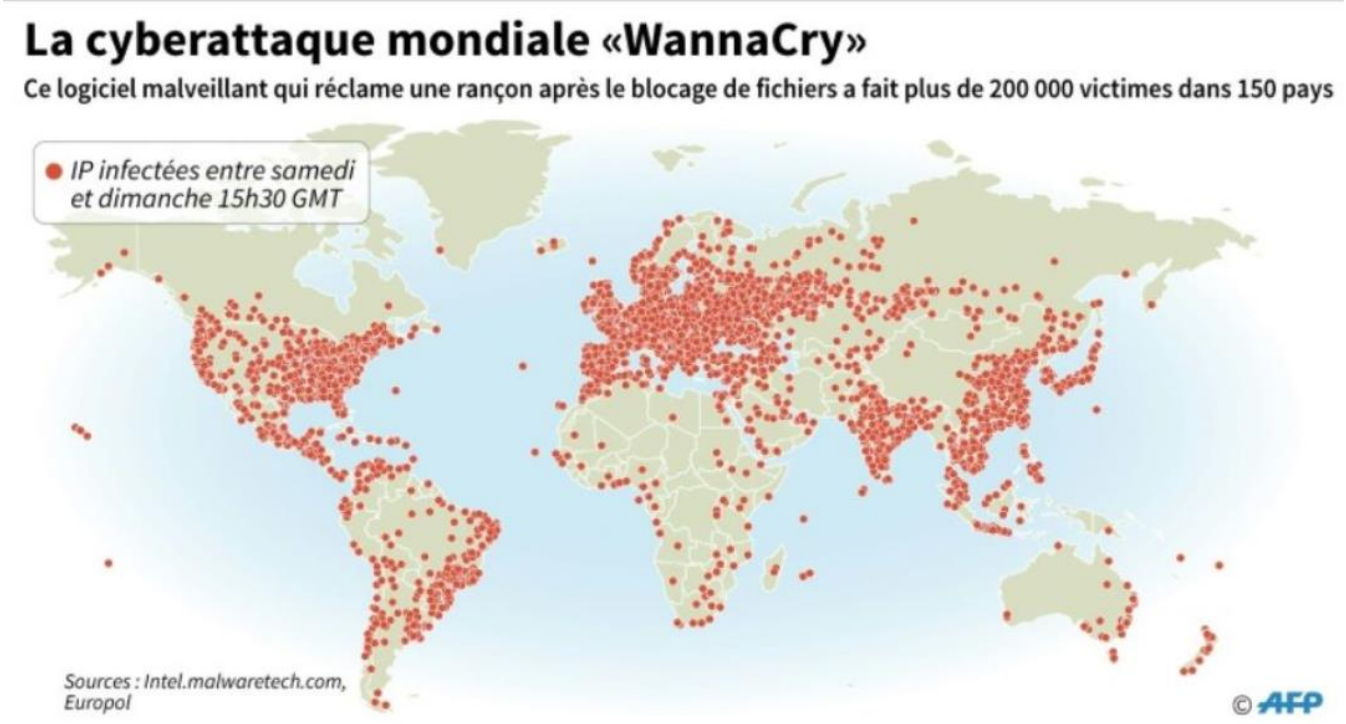
Depuis l'attaque « WannaCry » de mai 2017, les entreprises craignent une nouvelle cyber-attaque mondiale. Les organisations terroristes disposent de plus en plus de moyens matériels et financiers et pourraient, demain, utiliser cet angle d'attaque pour atteindre encore plus les entreprises et le public.

Les médias dénomment même les cyber-attaques comme « la nouvelle arme du 21e siècle »[30].

De plus, le fait de procéder à ce genre de mode opératoire pour attaquer une entreprise ou même plus largement un pays, est une activité très lucrative.

[30] Emission de radio RFI du 30 juillet 2017 – La cyber-attaque.

Le principe de rançon – « ransomware » – peut apporter un retour sur investissement de plus de 1000% aux pirates qui commettent les cyber-attaques[31].



Le Risk Manager a aussi une place prépondérante dans la gestion du risque terroriste en entreprise. Il est en effet nécessaire d'adopter une approche organisée et surtout globale au sein même de l'entreprise. Pour faciliter la mise en œuvre et l'intégration de cette démarche globale, il convient de se poser les bonnes questions : qui détient le risque ? Quelles sont les missions de chaque service/département à ce sujet ? Et donc, comment manager le risque conjointement ?

Le Risk Manager possède des compétences pluridisciplinaires. Il est donc en mesure de proposer des solutions en matière d'assurance et de prévention. Puis, il peut cartographier ces solutions pour illustrer ses idées et les soumettre aux autres fonctions (ressources humaines, sécurité/sûreté, comité directeur…). Le Risk Manager, face au risque terroriste, doit donc être convaincant, il doit réaliser également un travail de veille en amont pour récolter de la Data et être un « Risk Data ». Mais cela est plus marginal en Risk Management.

[31] Donnée chiffrée communiquée par Gérôme Billois, expert en cybersécurité chez Wavestone.

La collecte de données est davantage portée sur les sinistres, l'actualité législative et économique ou encore les retours d'expérience.

La spécificité majeure du poste de Risk Manager s'appuie sur le « crisis management » – ou gestion de crise en français. La mise en place de cellules de crise et l'organisation sous-jacente à ces dispositifs requiert une parfaite maîtrise de l'urgence et du stress. Ceci est familier pour le Risk Manager qui, au quotidien, traite des dossiers sinistres et participe à la gestion et à la résolution de situations de crise diverses et variées (présence de corps étrangers dans les matières premières, accidents, problématiques liées au transport ou à la Supply Chain etc…).

Pour mener à bien sa mission et maîtriser le risque terroriste, le Risk Manager, doit sensibiliser l'ensemble des collaborateurs, en adaptant son discours au niveau hiérarchique et à l'activité des collaborateurs.

Sa communication se veut responsable et non moralisatrice. Le Risk Manager apporte des éléments clefs pour prévenir le risque, il ne juge pas et ne diabolise pas le risque. Il permet aux collaborateurs d'être plus confiants et sereins ; ce qui leur permet d'être plus forts psychologiquement lorsque le risque se produit. Le Risk Manager va contribuer à l'assemblage des compétences de chacun pour pouvoir décliner des plans de maîtrise des risques structurés.

Après la sensibilisation, le Risk Manager prépare des actions plus techniques, et veille à mutualiser les risques. C'est le propre de l'assurance. Les couvertures assurantielles du risque terroriste sont aujourd'hui particulièrement développées, mais beaucoup d'entreprises ne s'assurent pas encore contre le terrorisme.

Pourtant, l'étendue des garanties pour les risques politiques au sens large en 2018 est très impressionnante : guerre étrangère, terrorisme, sabotage, grèves, émeutes, mutinerie, révolution, insurrection, actes de malveillance, rébellion, risques politiques, attentats, cyber-attaque, guerre civile… Ces garanties s'appliquent aux dommages matériels sur les actifs assurés et aux pertes d'exploitation subies suite aux dommages.

Le rôle des assureurs en 2018 dans la gestion du risque terroriste est de savoir s'ils doivent ou non intervenir. En effet, selon le pays concerné l'appellation « terrorisme » ne signifie pas la même chose qu'en France. Certains actes de violences d'ordre politique sont d'ailleurs qualifiés d'actes terroristes par les gouvernements. C'est pour cette raison que les entreprises privées et publiques auront besoin au cours des prochaines années d'une offre assurantielle large pour tous les types de violences d'ordre politique.

La couverture optimale devant prendre en compte les pertes d'exploitation et tous les types de dommages directs et indirects. La spécificité de la France est l'existence de deux fonds de garantie relatifs aux attentats terroristes : le GAREAT – Gestion de l'assurance et de la réassurance des risques attentats et actes de terrorisme et le FGTI – Fonds de Garantie des Victimes des actes de Terrorisme et d'autres Infractions.

Le GAREAT concerne les dommages matériels et a été créé en 2002 suite aux attentats du World Trade Center. Il est aujourd'hui considéré comme obsolète par un certain nombre d'entreprises qui demandent la révision de ce système.
Le FGTI est axé sur les victimes et sur les dommages corporels. Il a été instauré en 1986 suite aux attentats de la rue de Rennes à Paris.

B] UNE STRATEGIE GLOBALE

1) Le rôle de l'Etat

a. L'évolution du cadre juridique relatif au terrorisme

Le cadre juridique et réglementaire antiterroriste en France a évolué de manière très progressive depuis le milieu du XXème siècle. En effet, la menace terroriste a commencé à s'intensifier à partir des années 1970.

Il est devenu urgent de légiférer à ce titre. Les premières lois antiterroristes importantes sont entrées en vigueur en 1986 et en 1996. Ensuite, de nouveaux textes sont venus agrémenter et compléter les lois en vigueur.

Cette évolution législative est liée à la survenance de nouveaux attentats, en France comme à l'étranger. La loi du 9 septembre 1986, la première loi antiterroriste, commence par fixer le champ des actes relevant du terrorisme et en donne une définition précise. Il s'agit de la loi relative à la lutte contre le terrorisme et aux atteintes à la sûreté de l'Etat.

Pour le contexte, il est nécessaire de rappeler que cette loi a été votée seulement huit jours avant l'attentat de la rue de Rennes à Paris. Ce « célèbre » attentat a été perpétré pour le compte du Hezbollah et a fait 7 morts et 55 blessés en raison de l'ampleur de l'explosion. Ce fut donc le premier exemple d'application de la loi du 9 septembre.

Avec cette loi, toutes les affaires sont dès lors placées sous l'instruction de magistrats professionnels et de procureurs spécialisés dans la lutte antiterroriste. La section antiterroriste du parquet de Paris, la « quatorzième section », est créée au même moment grâce à ce texte. La spécificité du risque terroriste engendre la mise en place d'une exception notable : il n'y aura pas de juré à la cours d'assises de Paris pour le traitement de différentes affaires terroristes.

Plusieurs mesures majeures sont appliquées avec cette loi : le placement en garde à vue des suspects d'acte terroriste est étendu à quatre jours, les peines d'emprisonnement sont alourdies, faire l'apologie du terrorisme devient incriminable, des perquisitions peuvent être réalisées plus facilement aux domiciles des suspects, …

Enfin, un fonds de garantie, le FGTI[32] est créé pour les victimes d'actes terroristes, comme vu précédemment, suite à cet attentat de la rue de Rennes à Paris. Ensuite, les actes terroristes ont été insérés dans le nouveau code pénal à compter du 22 juillet 1992, ce qui permet de sanctionner encore plus lourdement ces actes. Mais l'évolution majeure suivante se fait avec la promulgation de la loi de 1996. Cette dernière renforce les textes et durcit les actions de prévention du risque.

Le placement en détention provision et les conditions de perquisitions (nocturnes notamment) sont assouplis, ce qui laisse davantage de marge de manœuvre aux forces de l'ordre et aux enquêteurs dans leur recherche des terroristes.

[32] FGTI : le fonds de garantie des victimes des actes de terrorisme

D'autres textes sont ensuite votés au début du XXIème siècle suite aux attentats du World Trade Center qui ont traumatisé le monde entier. Sans compter l'attaque terroriste à Madrid en 2004 et celle de Londres en 2005. Ainsi, le financement du terrorisme devient rapidement condamnable, la fouille des véhicules (lorsqu'ils se trouvent dans des aéroports, des ports, ou sur les routes) est plus aisée, le travail des enquêteurs est facilité avec la réduction de démarches administratives trop lourdes ou encore, les forces de l'ordre peuvent suivre la vie virtuelle d'un éventuel suspect (boîte mails, données d'accès aux réseaux etc..).

Ce dernier point montre l'évolution des modes opératoires des terroristes, qui utilisent davantage le digital et les nouvelles technologies au fur et à mesure des années. La loi la plus récemment adoptée est la « loi renforçant la sécurité intérieure et la lutte contre le terrorisme ». Elle a été promulguée le 30 octobre 2017 sous le Gouvernement d'Edouard Philippe. Elle vient renforcer les mesures relatives aux perquisitions et aux assignations à domicile, surtout pour les individus « fichés S ».

Malgré ce dernier renforcement législatif, les débats quant à la gestion de ces individus « fichés S » présents sur le territoire français sont particulièrement intenses. L'attaque au couteau du 12 mai 2018 à Paris ne peut que le confirmer. Les mesures législatives adoptées fin 2017 sont remises en question : comment un individu fiché S peut-il réussir à passer à l'action ? Qu'en est-il de leur suivi ?

A vrai dire, les fichés S sont plus de 10.000 en France. Il y a parmi eux des islamistes radicaux, des membres de courants d'extrême-droite, d'ultra-gauche, ou même des hooligans[33]. Le simple fait d'avoir côtoyé un individu appartenant à ces courants politiques et religieux peut faire de vous un individu fiché S. Une problématique se pose donc : ce fichier est-il réellement géré de manière optimale ?

Ce débat n'est pas l'objet de l'étude réalisée ici, cependant, ce contexte juridique peu efficient renforce et accroît le risque terroriste. Les entreprises sont donc de fait amenées à considérer ces éléments pour mettre en place des actions en interne. Les Risk Manager et les Directeurs Sécurité/Sûreté des entreprises privées doivent réaliser un travail de veille.

[33] Hooliganisme : mouvement d'adeptes du sport pratiquant l'exercice de la violence. (source de cette définition : « Hooligan » in World Wide Words)

Cet exercice exigeant et chronophage leur permet de prendre les bonnes décisions, et d'adapter leur politique interne selon les évolutions législatives et en fonction des vulnérabilités sous-jacentes à l'ensemble du cadre réglementaire établi.

Au niveau de la prévention, un plan gouvernemental nommé « Vigipirate » a été instauré en 1995 et est toujours actif à ce jour. Ce plan de prévention à grande échelle fixe des seuils de vigilance face à la menace et décrit les mesures de vigilance et de prévention qu'il faut appliquer si la menace s'amplifie. Il détermine également les responsabilités ainsi que les actions de l'Etat face au risque terroriste.

Plus récemment, une autre mesure a été mise en place : l'état d'urgence. Il a été promulgué et prorogé plusieurs fois jusqu'au 1er novembre 2017. Avant la série d'attentat de 2015, il avait été promulgué la dernière fois en 2005 suite aux émeutes dans les banlieues. L'état d'urgence permet une forme d'état d'exception (l'armée et les forces militaires ne sont pas impliquées contrairement à l'état de siège).

Avec l'état d'urgence, des mesures spéciales, restrictives, peuvent prises par les autorités. Les libertés sont réduites pour le bien de la société et la sécurité des civils. Les mesures prises peuvent être des interdictions de circuler, de porter une arme (malgré les autorisations détenues), de se rendre dans certains lieux publics, de manifester, … Selon le contexte, cela peut aller jusqu'à l'assignation à résidence.

En ce qui concerne les entreprises, elles détiennent des responsabilités et donc des obligations de sécurité et de sûreté. Cette responsabilité s'applique envers les collaborateurs, les visiteurs, les prestataires ainsi que les clients. Pour les salariés, il s'agit d'un devoir de protection des employés.

L'entreprise doit prendre toutes les dispositions nécessaires pour garantir la sécurité et la protection de la santé physique et mentale de ses employés. L'entreprise est détient une obligation de résultat qui doit se traduire par des actions réelles et tangibles. Ce devoir de protection s'applique aussi aux visiteurs, aux prestataires/fournisseurs ainsi qu'aux les clients.

De facto, l'entreprise a une responsabilité de sécurité vis-à-vis de personnes externes également. Les sites ouverts au public sont donc soumis à un défi de sûreté et de sécurité

très important puisque les tiers sont difficilement maîtrisables. Au sein de Nestlé France, c'est l'entité Nespresso qui est fréquemment confrontée à ce type de problématiques. Avec près de 70 boutiques sur le territoire français, toutes placées à des endroits stratégiques et prestigieux (Champs Elysées et quartier du Marais à Paris notamment), Nespresso est vulnérable face au risque terroriste. Les collaborateurs de Nespresso reçoivent par ailleurs une formation en interne dédiée à la sûreté. Parallèlement, une forme de partenariat a été créée avec le RAID[34] pour organiser une fois par an, des exercices d'évacuation et de confinement. Encore une fois, le lien et la communication avec d'autres acteurs permet de lutter contre la menace efficacement.

b. Le soutien de l'Etat

Lorsque plusieurs professeurs de l'école nationale d'assurance sont interrogés au sujet de l'intérêt de la gestion du risque terroriste par les entreprises, ils répondent en majorité que « la gestion de ce risque est du ressort de l'Etat »[35]. Le risque terroriste est un risque d'origine humaine, un « act of devil ». Il est donc tout à fait légitime d'associer la gestion de ce risque aux fonctions régaliennes ; leur pouvoir étant théoriquement plus important que celui des autres acteurs économiques – dont les entreprises. Cependant, les éléments développés au long de la présente étude permettent d'affirmer que la gestion du risque terroriste se doit d'être globale pour être mieux maîtrisée.

Même s'il s'agit d'un sujet tabou, on ne peut aujourd'hui déresponsabiliser un acteur économique tel que les entreprises et maintenir une stratégie d'évitement du risque terroriste en en confiant exclusivement sa gestion à l'Etat. Tous les acteurs économiques ont un rôle prépondérant dans cette gestion, il ne s'agit pas là uniquement d'une problématique géopolitique, militaire ou politique.

[34] Unité d'élite de la police nationale française : RAID pour Recherche, Assistance, Intervention, Dissuasion.
[35] Question posée en novembre et en décembre 2017 à plusieurs professeurs de l'école nationale d'assurance : Les entreprises ont-elles un rôle à jouer dans la gestion et la prévention du risque terroriste ?

En effet, les outils régaliens sont saturés en cas de pluri-attentats, c'est ce qui a été constaté dans la plupart des retours d'expérience des attaques de 2015.

Aussi, la vie économique est touchée par ces menaces intérieures, sans compter l'impact psychologique sur l'ensemble de la population qui est très sensible à ce risque. Le secteur privé doit donc s'adapter à ce contexte en assurant, parallèlement aux actions de l'Etat et des autres acteurs économiques, une gestion de ce risque à son échelle.

Le Risk Manager ne doit pas changer le monde mais le manager à l'optimum. Il va rassurer et donner la confiance à l'ensemble des salariés de l'entreprise en mettant en place des mesures de protection, des mesures de réaction ainsi que des mesures de formation adéquates.

Le rôle de l'Etat est davantage axé sur la gestion en aval qu'en amont de ce risque : indemnisation des victimes, soutien public et communication nationale et internationale. Les forces de l'ordre sont au cœur de la protection puisqu'ils interviennent sur la réduction et la minimisation du risque. Et, les services de renseignement, les Risk Managers et Directeurs Sécurité/Sûreté des entreprises, interviennent davantage en amont, en employant des mesures de prévention pour anticiper, réduire ce risque.

Depuis les attentats de 2015, l'Etat agit également en amont afin d'aider la population à adopter les bons comportements en cas d'attaque terroriste. Le gouvernement a mis en place un site internet dédié au risque terroriste et a développé une campagne de communication.

Cette campagne s'est essentiellement appuyée sur des bonnes pratiques transcrites par des affiches ou des flyers. L'annexe 1 est un exemple d'affiche créée et diffusée à l'issue des attentats de janvier 2015.

Aussi, sur le site internet du gouvernement, il y a la possibilité de « dénoncer » un individu potentiellement radicalisé. Des conseils d'observation sont également donnés pour identifier la menace.

Le gouvernement a un rôle davantage axé sur la protection et la stratégie en cas d'attaque terroriste. Son action est plutôt « macro » puisque l'Etat dispose d'informations globales et doit avant tout protéger le pays plutôt que les personnes individuellement.

Cela passe par des actions comme la protection des OIV. Les OIV sont les opérateurs d'importance vitale. Ils sont définis précisément dans le code de la Défense aux articles L. 1332-1 et L. 1332-2. Ce sont en fait des opérateurs publics ou privés qui exercent des activités dites « vitales ». La destruction ou le sabotage de l'une de ces activités par un acte de malveillance ou de terrorisme pourrait avoir un impact sur le pays tout entier. Ce pourrait être des conséquences sanitaires ou économiques.[36]

Les opérateurs d'importance vitale sont donc des membranes de la stratégie de sécurité nationale. Pour des raisons de confidentialité et de sécurité, les noms des opérateurs d'importance vitale ne sont pas communiqués. Néanmoins, le gouvernement permet de savoir dans quels secteurs d'activités ils se trouvent : la santé, le transport, la gestion de l'eau, l'industrie, l'énergie, la finance, la communication, les activités militaires, les activités civiles de l'Etat, les activités judiciaires, l'alimentation, la recherche. Soit 12 domaines où les opérateurs d'importance vitale exercent, ce qui est particulièrement large et varié.

Au total, on dénombre 249 opérateurs d'importance vitale en France, ce sont des entreprises du secteur public et du secteur privé. Toutes ces entreprises ont des activités qui ne sont ni remplaçables ni substituables (ou du moins, très difficilement). De fait la protection de ces opérateurs est réalisée de manière structurée et précise. Plusieurs ministres sont rattachés à la coordination de la protection des activités vitales. Les secteurs d'activités étant très divers, un seul ministre ne pourrait être en mesure d'orchestrer cela. Il est possible de nommer quatre catégories majeures parmi toutes les activités précitées : la dimension humaine, la fonction régalienne, l'activité économique du pays et la dimension technologique.

Une politique de sécurité des activités d'importance vitale appelée « SAIV » est appliquée et mise à jour régulièrement. Les textes sur lesquels elle se base sont appelés des « Directives nationales de sécurité ». Ces Directives nationales de sécurité, « DNS », sont rédigées par les ministres coordonnateurs selon chaque domaine et chaque sous-domaine d'activité.

Les DNS décrivent les enjeux du secteur, les forces et les faiblesses ainsi que les menaces potentielles. L'objectif de ces directives est d'identifier comment protéger l'opérateur d'importance vitale. Ensuite, chaque opérateur définit des « PIV » à savoir des points

[36] Définition reformulée et simplifiée des articles L.1332-1 et L.1332-2 du Code de la Défense.

d'importance vitale. Il s'agit de zones indispensables à la vie du pays. Des bâtiments, des établissements, des activités ou des encore des installations indispensables.

En clair, ce sont notamment des points de réseau tactiques, des sites de production ou encore des centres informatiques. Tout s'articule enfin autour des textes (SAIV et DSN) et des acteurs clefs de la sécurité nationale : le premier ministre et le secrétariat général de la défense et de la sécurité nationale (SGDSN) qui conçoivent et pilotent l'ensemble du dispositif, les ministres coordonnateurs, le ministère de l'intérieur, les préfets de zone de défense et de sécurité ainsi que les préfets de département et les opérateurs d'importance vitale.

Ce qu'il faut retenir de cette solide organisation est le statut spécifique attribué aux opérateurs d'importance vitale. Ils sont au centre de tout le dispositif mis en place et peuvent réaliser des requêtes spécifiques. Il s'agit par exemple de requête de criblage afin d'obtenir des informations sur l'identité et les caractéristiques d'un individu donné. Si l'opérateur d'importance vitale identifie une menace, il peut obtenir des informations confidentielles, surtout si c'est un point d'importance vitale est menacé.

Cela permet de préserver les sites stratégiques des opérateurs d'importance vitale. Au-delà de cette obtention d'informations clef, un collaborateur de l'entreprise est délégué à la défense et à la sécurité. Cela permet d'avoir un lien avec l'autorité administrative et d'avoir un interlocuteur unique habilité « Confidentiel défense ». L'Autorité pourra échanger avec ce délégué de l'entreprise OIV et lui communiquera les éventuelles modifications du dispositif Vigipirate.

2) Le cas des entreprises établies sur le plan international

a. Les entreprises du secteur tertiaire

Le secteur tertiaire représente la production des services. Cela va de la mise à disposition d'une capacité technique (services juridiques, d'architecture, de coiffure, de blanchisserie...) aux transports, en passant par l'administration, le commerce, les activités financières et immobilières, les services aux entreprises et aux particuliers, l'éducation, la santé et l'action

sociale[37]. Cet ensemble représente près des trois quarts de la valeur ajoutée et des emplois comptés en équivalent temps plein de la France. L'impact du risque terroriste va varier en fonction du secteur d'activité de l'entreprise, de sa notoriété, de son exposition sur le plan international ou encore de sa culture d'entreprise et des symboles qu'elle véhicule.

Il n'y a pas de liste exhaustive aux critères et caractéristiques pouvant augmenter ou réduire ce risque. Cela dépend de l'attaque subie, de l'organisation terroriste en question qui va commettre l'attaque mais aussi du pays et/ou de la zone où l'événement se produit. Les conséquences humaines sont les plus délicates à traiter, tant en amont qu'en aval. Mais on évoque peu dans la presse et les médias les risques inhérents aux actifs de l'entreprise et à son cœur d'activité – *id est* le « business ». Les actifs de l'entreprise comprennent tous les biens et les droits que possède l'entreprise: les bâtiments, les fonds de commerce, le matériel, les créances, les brevets déposés, etc…[38]

Ainsi, il peut s'agir soit de risques politiques pouvant impacter directement les actifs ou bien de risques de zones ; notamment dans les zones touristiques. Cette notion d'actif est étendue au patrimoine de l'entreprise au sens large. On peut donc y intégrer les conséquences sur l'image de l'entreprise ou le risque d'information.

Ces problématiques d'image et d'information sont sensibles et sont, souvent, traitées par les responsables de l'ERM, Enterprise Risk Management, de la société. L'ERM est une démarche « top-down », allant du sommet de la hiérarchie de l'entreprise vers le bas. Le top-down se focalise sur les risques stratégiques, tactiques, opérationnels et de conformité (c'est la méthode « STOC » en anglais). L'Enterprise Risk Management, et donc le « top-down », découle du CEO[39] et du CRO[40].

Cette méthode permet de considérer toujours l'entreprise dans son ensemble, les risques dans leur ensemble. C'est une vision globale des risques qui prend également en compte les dimensions stratégiques et ne se perd pas dans le détail. C'est là que sont prises les grandes décisions en termes de risques.

[37] Définition Alternatives Economiques – numéro 53 – Janvier 2011.
[38] Définition du service public - Direction de l'information légale et administrative.
[39] CEO: C*hief Executive Officer* en anglais. Traduction : Directeur Général.
[40] CRO: Chief Risk Officer en anglais. Traduction : Directeur des Risques.

Pour les entreprises du secteur tertiaire qui exercent à l'international, les domaines d'activités (et donc les impacts et conséquences probables) sont très variés. Mais parmi tous les secteurs d'activités, ce sont les transports qui sont le plus touchés par le risque terroriste au-delà des frontières. En effet, tous les échanges à travers le monde sont dépendants des transports et plus précisément des activités maritimes et aériennes.

La conjoncture économique mondiale des dernières décennies et la mondialisation au sens large sous-entendent des flux importants de marchandises, de biens, de services et de personnes. Le but de ce domaine d'activité est de dynamiser l'économie mondiale par les imports et les exports. Tous les modes de transport, qu'ils soient du domaine maritime, terrestre, aérien ou encore fluvial sont très vulnérables au risque terroriste. En effet, les flux sont complexes et la sécurité sur certains trajets reste parfois peu élevée.

Les navires peuvent être attaqués et leurs cargaisons endommagées ou volées (selon le type de cargaison transportée). Les transports sont aussi sujets aux fraudes puisque les organisations terroristes établissent fréquemment de faux documents pour se procurer des moyens de transports (camions, navires, etc…). Aussi, les marchandises transportées dérobées par les organisations terroristes servent de ressources aux terroristes et leur permet de financer leurs activités. En effet, les marchandises transportées à travers le monde sont très diverses.

En s'attaquant aux transports, les terroristes peuvent se fournir une large gamme de produits, de matériaux et d'équipements. C'est surtout le transport terrestre qui est touché par le terrorisme. Cela s'explique par le fait que les itinéraires empruntés par les camions sont facilement accessibles. Contrairement aux airs ou aux mers, l'ensemble des routes n'est pas placées sous surveillance. Il est parfois même difficile de retrouver d'obtenir des images issues de caméra de surveillance sur les autoroutes européennes.

De fait, les terroristes peuvent emprunter les ponts, les tunnels, les aires de repos pour dérober des véhicules, des utilitaires ou des camions…et leurs marchandises.

Aussi, les entreprises qui exercent dans le domaine du transport savent que leur exposition au risque terroriste peut être aggravée si le mode de transport utilisé identifie le pays d'origine du transporteur. Par exemple, si les terroristes cherchent à atteindre la France, ils vont chercher à atteindre un transporteur français.

Il existe d'autres facteurs qui vont aggraver l'exposition au risque terroriste, notamment : les zones géographiques où vont se dérouler les transports de marchandises, le type de marchandises transportées (s'il s'agit d'armements, de métaux ou d'équipements informatiques.. le risque sera plus accru) ou encore, le moyen de transport utilisé (un aéronef pourra être utilisé pour réaliser un attentat, ce fut le cas lors des attentats du World Trade Center).

L'objectif premier des terroristes est de provoquer un maximum de pertes, plus les conséquences sont lourdes et plus la terreur sur les populations est importante. *De facto,* les attaques terroristes envers les entreprises de transport sont soit stratégiques ou tactiques – pour étayer leurs activités, s'équiper ou préparer un attentat – soit il s'agit d'attaques « finales » où le but est de provoquer des pertes matérielles et humaines très fortes.

Cette menace très pesante sur les entreprises de transport a conduit la plupart des Etats à fixer des prérogatives pour engager une réduction du risque terroriste. Ce sont les transports terrestres et maritimes qui, comme vu précédemment, sont les plus sensibles à la menace et plus facilement atteignables. Les Etats ont initié des mesures de prévention et de protection puis, plusieurs organisations internationales ont suivi cette démarche pour créer des textes internationaux. C'est le cas de l'OMI, l'organisation maritime internationale qui a étendu ses politiques de sécurité en 2004 en renforçant les équipements et installations nécessaires dans les ports. Cela correspond à une extension des normes déjà en vigueur à savoir la convention SOLAS et la convention de 1974 avec, pour la France l'obligation de mettre en place des plans de sûreté.

En parallèle, l'Europe et les Etats-Unis ont signé un accord appelé CMAA (accord de coopération douanière et d'assistance mutuelle) pour apporter un socle plus solide aux accords de coopération douanière existants et sécuriser davantage la Supply Chain (chaîne logistique). Aussi, en France, les différents niveaux de sûreté fixés par les textes ont été mis en conformité avec le plan Vigipirate.

Toutes les dispositions adoptées représentent des coûts financiers très élevés pour les Etats et les organisations internationales qui les ont mises en place. Cependant, elles apportent des atouts importants puisque les ports et aéroports se sont modernisés.

Ceci a permis une réelle diminution de l'exposition au risque terroriste mais pas que : piraterie, vol et détournement de marchandises entre autres, sont aussi des risques qui ont été réduits. De fait, les polices d'assurance des entreprises de transport ont eu un impact très positif en commençant par une réduction des primes avec la baisse de sinistres constatés.

b. Les industries : focus sur l'industrie agroalimentaire (Nestlé France)

Nestlé France est une grande entreprise bien implantée en France qui détient des activités internationales. Nestlé est surtout une multinationale, le leader mondial de l'agroalimentaire. Comme d'autres grandes entreprises, elle est particulièrement exposée au risque terroriste puisque la menace n'est plus exogène mais bien endogène, depuis les attentats de 2015.

Au total, pour les entreprises françaises, il existe 40.000 filiales françaises implantées sur tous les continents. Les entreprises plus petites, les ETI à contrôle français[41], sont elles aussi exposées au risque terroriste puisqu'un tiers d'entre elles sont justement implantées à l'étranger. Nestlé France lie un certain nombre de partenariats avec ce type d'entreprises, qui deviennent ses clients et fournisseurs.

Dans ce contexte, un point d'honneur est mis sur la Sécurité/Sûreté dans chaque entité Nestlé sur la planète. Comme la Sécurité/Sûreté, le Risk Management est étendu pour chaque marché de Nestlé dans le monde, dont le marché français, afin de tenir compte des spécificités locales.

Il est parfois difficile d'imaginer le nombre de marques commercialisées sur le marché français qui appartiennent à Nestlé. Le schéma ci-après permettra au lecteur de prendre conscience des enjeux économiques et financiers de Nestlé en France. L'appréhension de la vulnérabilité de Nestlé France face au risque terroriste en sera ensuite plus aisée.

[41] ETI : entreprise de taille intermédiaire ; qui a entre 250 et 4999 salariés.

Chez Nestlé France, les différents départements qui traitent les sujets de sûreté travaillent conjointement sur des problématiques communes dont celles liées au terrorisme, aux actes de malveillance mais aussi aux sinistres automobiles par exemple, en cas d'utilisation de véhicules comme d'une arme par un tiers ou un collaborateur.

Au-delà du département Risk Management français et de la direction Sécurité/Sûreté, des « Security Champions » sont intégrés au sein de chaque site Nestlé en France. En effet, les postes de Risk Manager ou de Directeur Sécurité/Sûreté sont basés au siège social de Nestlé France. La mise en place de Security Champions a permis d'affecter des interlocuteurs uniques sur le terrain. Ce concept de Security Champion provient des Etats-Unis. Le terme « champion » n'est pas entendu sous le sens de performance sportive mais bien comme un porteur de philosophie, un modèle dont on s'inspire.

Le Security Champion est un salarié, un membre d'une équipe projet ou un représentant de site qui a sa charge les questions de sécurité. Il communique les messages importants de la direction Sécurité/Sûreté et Risk Management aux collaborateurs qui l'entourent, et il doit

apporter des réponses rapidement aux questions émanant des salariés. C'est un intermédiaire, un interlocuteur clef de la sécurité au XXIème siècle puisque les Security Champions sont formés, entre autres, aux cyber-risques. Au sein de Nestlé France, les Security Champions sont en charge des questions relatives à la fois à la sûreté et à la sécurité.

En cas de crises, d'attaques terroristes ou d'actes de malveillance sur un site de production ou de distribution de Nestlé, le Security Champion du site sera au cœur des échanges avec le siège social et donc des décisions stratégiques. La responsabilité de Security Champion a été créée en 2016. Cela a représenté un long programme de développement notamment pour les usines. Il a fallu que les départements SHE (sécurité, hygiène et environnement), Qualité, Risk Management, Sécurité/Sûreté ainsi que les Achats désignent les salariés à même de pouvoir représenter des modèles en termes de bonnes pratiques de sûretés et de sécurité.

Après cette phase de désignation, les salariés dénommés Security Champions ont suivi des périodes formation dans différents centres de compétences Nestlé (essentiellement au siège social) afin de posséder toutes les connaissances et compétences nécessaires pour être des acteurs de la sécurité au quotidien. Ce « titre » de Security Champions est une forme de certification interne, qui vient s'ajouter à l'activité, au métier exercé au quotidien par le collaborateur. Les collaborateurs sont choisis après avoir établi une candidature.

Depuis le début de l'année 2018, plusieurs Security Champions peuvent être établis sur un même site. Cela permet de renforcer les bons comportements sécuritaires sur le terrain, de partager leurs expériences et surtout de bénéficier d'un « back-up », c'est-à-dire d'une continuité de la mission, y compris en cas d'absence d'un des Security Champions. Il est considéré au sein de Nestlé que ce programme de Security Champions est une réussite.

En effet, le taux d'attaques, d'actes de malveillance et d'incivilités a fortement diminué depuis deux ans. Il en est de même pour l'accidentologie sur sites : aucun accident corporel n'a été relevé au cours de l'année 2017. Le Security Champions a cette « double casquette » de risques : il est référent tant pour les risques inhérents à la sécurité qu'à la sûreté. Il est donc amené à être formé à la prévention et à la gestion du risque terroriste en entreprise.

Au niveau global, les objectifs de la politique Sécurité/Sûreté de Nestlé France consacrés à la prévention et à la gestion du risque terroriste à l'aube 2022 sont en partie fixés par la zone Nestlé en Europe.

Ils sont discutés et étayés par la Direction Générale de Nestlé France et par l'ensemble des Responsables de Nestlé qui œuvrent sur des problématiques de Sécurité/Sûreté. Ils s'articulent sous trois axes.

Le premier axe s'appuie sur la diffusion d'informations relatives à la sécurité/sûreté et à la création d'une culture de la sûreté dans l'entreprise. Cela consiste à créer et à maintenir un environnement de travail sûr et sécurisé, grâce à la mobilisation et à l'appui des collaborateurs en vue de contribuer à la prévention des risques.

Le renforcement de la culture de la sûreté passe par le déploiement d'un programme de sensibilisation appelé « NGS » pour Nestle Group Security. Il s'agit d'un « Security Awareness program », un programme de sensibilisation à échelle européenne qu'il faut adapter aux caractéristiques du marché français. Il est composé de nombreux outils de communication, de bonnes pratiques et de documents, à usage interne, pour accompagner les membres de la Sécurité/Sûreté et du Risk Management à toutes les échelles. Mais aussi, d'objectifs à fixer ou non selon le pays concerné ou à modifier. Il s'agit notamment du fait de disposer d'une structure et d'un processus sûreté dans chaque site.

Cela correspond au fait d'avoir un comité local pour suivre les thématiques liées à la malveillance sur le site, de détenir une procédure locale pour définir le rôle, les missions et les responsabilités des acteurs de la sûreté sur le site ou encore, de bénéficier d'un Guide des recommandations pour la protection de la chaine alimentaire.

Ce dernier point fait référence à l'intégration de questions de Food Defense. Le Food Defense, ainsi que le Food Fraud correspondent à la protection de la chaîne alimentaire contre les risques d'actes malveillants, criminels ou terroristes. Ce sont des concepts bien connus des industriels, surtout depuis les attentats du World Trade Center le 11 septembre 2001.

En effet, depuis cet événement clef de la gestion et de la prévention du risque terroriste, d'innombrables scenarii ont été pensés et imaginés. Dans le cadre du secteur de l'agroalimentaire, le risque de contamination accidentel a toujours été estimé. Il s'agissait donc d'une problématique de sécurité.

En revanche, c'est bien depuis les attentats du World Trade Center que les industriels ont songé aux actes volontaires de contamination des produits alimentaires et des matières. Ce qui en fait une problématique de sûreté. Selon le référentiel de l'IFS – International Features Standards – 70% à 80% des problématiques de Food Defense proviennent d'actes de contamination réalisés par les membres du personnel directement présents sur les sites où se trouvent les lignes de production.

Ces actes peuvent résulter d'une forme de mécontentement, d'une forme de militantisme quelle qu'elle soit ou pire, d'une volonté de nuire à la santé des consommateurs. Dans tous les cas, les conséquences pour l'image de l'entreprise peuvent être lourdes. La menace terroriste dans l'agroalimentaire est bel et bien réelle. La gestion de l'hygiène en usine, dans la manipulation et le traitement des matières premières et des aliments est particulièrement développée aujourd'hui. Aussi, les produits sont sécurisés et vérifiés à multiples reprises avant de quitter le centre de production.

Et Surtout, l'offre sur le marché est particulièrement abondante, la concurrence est plus qu'exacerbée dans le domaine de alimentaire. Ainsi, un produit alimentaire atteint par une contamination serait facilement substituable. Alors, pourquoi le risque terroriste, ou plutôt le bioterrorisme, reste-t-il envisageable ?

L'alimentation reflète une symbolique à laquelle les consommateurs pensent peu : la nourriture est connotée à la gourmandise dans certains textes religieux et donc aux notions de plaisir et de confort. C'est une cible à prendre très au sérieux puisque l'acte bioterroriste peut être accompli à moindre coût, par la contamination de sources d'eau potables, de matières premières ou plus largement par la contamination des services de restauration d'établissements hôteliers ou de grands restaurants.

Ces derniers restent moins sécurisés que les ambassades ou les structures militaires, et pourtant le nombre de victimes potentielles serait très élevé. Aux Etats-Unis, les sujets du bioterrorisme ou de l'agroterrorisme sont connus et appréhendés depuis le début des années 2000.

Le bioterrorisme correspond à l'incorporation délibérée de toxines ou de germes dans des produits à destination de l'alimentation humaine. L'agroterrorisme concerne quant à lui l'insertion d'agents dans des récoltes qui vont causer leur perte.

L'agroterrorisme va créer un blocage, une suspension de la production alors que le bioterrorisme va atteindre directement la santé et la vie des populations. Au sein du référentiel IFS, les conditions à appliquer pour protéger au mieux les entreprises agroalimentaires de ce type d'attaques sont détaillées.

Au cours des audits des sites, comprenant l'évaluation des risques et des plans d'actions en vigueur, les standards de Food Defense sont évalués, ce qui donne lieu ou non à l'obtention d'une certification. Ceci permet de challenger les usines et autres sites de production alimentaires sur les questions de sécurité et de sûreté. C'est un bon point d'ancrage pour sensibiliser les collaborateurs aux vulnérabilités du domaine de l'agroalimentaire face au risque terroriste.

Le deuxième axe relatif aux objectifs de la politique Sécurité/Sûreté de Nestlé France pour 2022 s'appuie sur l'amélioration de l'intégration de la sûreté dans le « business ». Cela correspond au fait d'assurer la cohérence des normes et standards Nestlé. C'est également le fait de s'assurer que les prestations de sécurité et de sûreté soient optimisées (en termes de ratio moyens/coûts). Il est primordial dans cette démarche globale de vérifier que les fournisseurs soient dans chacun des pays à la fois conformes, éthiques et transparents.

Le suivi des prestataires doit être réalisé trimestriellement pour les prestataires de surveillance humaine. D'ailleurs, des KPIs[42] sont mis en place pour évaluer la prestation de ces services. L'objectif est d'obtenir une garantie du sérieux des fournisseurs. C'est une vérification régulière des actions réalisées par ces derniers. Des KPIs positifs illustrent le fait que les prestations soient toujours conformes aux demandes initiales de Nestlé France. Ces demandes étant établies dans le contrat local initial (signé entre le prestataire des services de surveillance d'une part et par Nestlé d'autre part).

En revanche, si les KPIs sont peu satisfaisants et/ou si le contrat de prestation atteint sa date d'échéance, il faut réfléchir à la reconduction du contrat ou bien à la préparation d'un nouvel appel d'offres. Cela est essentiel pour bien intégrer les processus de sûreté au cœur du business, en garantissant des services de protection optimaux.

[42] KPIs : les Key Performance Indicators sont en français, les indicateurs clés de la performance. Ils sont mesurés de manière qualitative et/ou quantitative. Ils permettent l'évaluation d'un service ou d'une prestation.

Le meilleur moyen de confirmer la qualité des services de surveillance humaine et d'évaluer le niveau de protection d'un site est de procéder à un audit de sécurité et de sûreté. Par contre, dans les chantiers d'amélioration de la protection des sites fixés, il y a un plusieurs actions à mener après l'audit. Selon les normes et standards Nestlé pour l'audit interne, il s'agit d'établir l'état des besoins, de recevoir des informations et surtout de challenger les propositions reçues, de les mettre en œuvre, et enfin de les maintenir. Ce travail chronophage devient efficace dès lors que tous les parties prenantes à la protection du risque travaillent et échangent ensemble sur ce sujet.

Le troisième et dernier axe est le renforcement de la sûreté dans le management des risques. Cet objectif est consacré au Risk Management et adapte les grandes étapes de la gestion du risque aux spécificités du risque terroriste. C'est l'identification systématique des individus (notamment par le système de badge multifonctions, cf. Annexe 4), l'évaluation, la hiérarchisation et la gestion des risques de sûreté. Pour faire face à ces enjeux, le Risk Manager va vérifier et améliorer le niveau de préparation de crise en cas de problème lié à la sûreté. Il va veiller à améliorer la gestion des risques de fraudes et se questionner sur les problématiques de sûreté dans le transport et la Supply Chain (chaîne logistique).

En effet, Nestlé France transporte un nombre de marchandises considérables au quotidien. Nestlé Waters France, par le biais de ses usines de Vittel et Vergèze, exporte toutes les eaux Nestlé à travers l'Europe. Les incidents doivent être remontés trimestriellement et ce quel que soit leur nature (dégradations, vols, pertes etc.). Une évaluation du préjudice subi est réalisée à chaque fois. Mais une priorité est donnée aux urgences opérationnelles.

Tous ces éléments seront constitutifs d'un rapport sur l'exposition au risque de sécurité et de sûreté avec une partie détaillée sur le risque terroriste. La forme adoptée est un reporting détaillé pour une meilleure compréhension de tous les collaborateurs.

Le transport des marchandises est, comme vu en partie B-2.a, un des domaines les plus exposés au risque terroriste. Le sous-jacent du panorama de marques de Nestlé commercialisées en France est la structuration de ses flux de marchandises et de matières premières. Les équipes Sécurité/Sûreté et Risk Management de Nestlé sont conscientes de la vulnérabilité de l'entreprise face à ce risque et ont, de fait, mis en place un dispositif intégré permettant de suivre toutes les problématiques liées au transport.

Il s'agit du TMS, pour Transport Management System. L'ensemble des marques sont englobées depuis plusieurs années dans ce dispositif, hormis Herta et Nestlé Waters, qui sont intégrées progressivement. Les flux de ces deux dernières marques sont tellement importants que leur digitalisation se réalise sur plusieurs années.

D'ici à 2020, tous les flux de marchandises et de matières premières de Nestlé France pourront être suivis en direct via Internet par l'équipe Sécurité/Sûreté, Risk Management mais aussi les Achats et les services Qualité. A ce jour, c'est donc plus de 90% des flux qui sont enregistrés, ce qui est déjà une belle performance. Cet outil est un allié précieux pour la sécurité et la sûreté des transports entrants et sortants.

En effet ce système qui repose sur une plateforme d'accès sécurisé qui permet l'échange d'informations entre le Chargeur, le Transporteur et le Receveur. Pour le Chargeur et le Receveur, les données enregistrées vont être les suivantes : nom du chauffeur, numéro du tracteur et/ou de la remorque, nom et coordonnées du sous-traitant, numéro du plomb etc…

Aussi, ce qui est particulièrement intéressant est le fait que le chargeur reçoive une notification sur son smartphone lui indiquant s'il le camion qu'il va charger est le bon ou non. Cela permet d'éviter un certain nombre d'erreurs fréquentes dans les chargements et surtout d'éviter la fraude et donc de contrer la menace terroriste à la source.

Pour le Transporteur, d'autres informations importantes apparaissent comme le nom des sites de chargement et de déchargement, ainsi que les informations clefs nécessaires au chargement : le nombre de palettes, le poids total, le volume, le bon de livraison et le titre de transport.

Tous les sites de production Nestlé sont certifiés « NQMS » pour Nestle Quality Management System. Ils détiennent également d'autres certifications comme ISO 9001 (Qualité), ISO 14001 (Environnement), OHSAS 18001 (sécurité) et FSSC 22000 (sécurité des denrées alimentaires). Dans le cadre des programmes de reconnaissance mutuelle entre les différentes certifications,[43] depuis le 31/10/2013, les auditeurs sont également invités à considérer la partie Food Defense.

[43] Certifications ISO 22000, FSSC, IFS et BRC.

Pour rappel, cette dernière couvre les risques de dégradation volontaire et malveillante des denrées alimentaires. Ce sont soit des risques internes (de type sabotage) soit des risques externes (de type terrorisme). Lors des audits d'usines, le sujet Food Defense ressort fréquemment. Les auditeurs sont donc sensibilisés à ce sujet.

L'audit consiste en une vérification documentaire et terrain. De fait, les auditeurs attendent une analyse documentée des risques internes et externes de dégradation volontaire malveillante des denrées. Il s'agit d'un modèle standard pour tous les sites de Nestlé France à adapter par site. A noter que l'auditeur ne peut pas exiger que cette analyse soit intégrée dans le HACCP de l'usine. Le HACCP correspond à un outil d'évaluation des menaces. En anglais, cela signifie : « hazard analysis critical control point » pour l'analyse des dangers et des points critiques.

C'est un point bien distinct de l'analyse de Food Defense bien que le Food Defense y soit intrinsèquement lié en tant que menace et danger pour l'entreprise. Les auditeurs attendent aussi de la part des sites des preuves que les risques sont maitrisés (qu'il y a des « éléments en place ») ou que des actions correctives sont planifiées pour fermer les écarts. Les éléments en place sont des Prérequis (PRP en langage Qualité) pour éviter que les risques atteignent des niveaux inacceptables.

A l'issue des audits, plusieurs recommandations sont faites aux usines pour améliorer leur protection. La première recommandation faite aux responsables Qualité des usines est de ne pas tenter de répondre seuls aux questions des auditeurs mais de s'appuyer sur leur Security Champion en cas de question sur ces sujets. Ensuite, les diverses recommandations émises sont classifiées et hiérarchisées selon leur type de risque.

Rien n'est obligatoire mais si l'année suivante, les recommandations n'ont pas été suivies, le site peut perdre sa certification. De nombreux assureurs exigent l'obtention et le maintien des différentes certifications précitées pour pouvoir couvrir le risque. C'est le cas des assureurs de Nestlé France qui souhaitent détenir un minimum de garanties sur le risque assuré compte-tenu de la vulnérabilité de l'entreprise face au risque terroriste et aux risques de Sécurité/Sûreté au sens large.

En effet, plusieurs cas de contaminations volontaires et malveillantes ont été relevés en France au cours des vingt dernières années dans le domaine alimentaire.

Nestlé fut touché dans le passé avec la marque Perrier. En 1990, du benzène, un gaz cancérigène, a été trouvé dans les eaux et le scandale a été colossal pour la marque et pour Nestlé dans son intégralité. 280 millions de bouteilles ont été rappelées, le chiffre d'Affaires de la marque a chuté de 35% l'année suivante.

Plusieurs médias ont indiqué à l'époque qu'il s'agissait d'une erreur humaine, que les équipements filtrant les eaux de Perrier n'avaient pas été changés en temps et en heure. Cela n'a jamais été validé par les équipes Qualité de Nestlé, qui n'ont d'ailleurs jamais réussi à identifier l'origine de cette contamination.

Depuis cet événement, les processus qualité, sécurité et sûreté sont très prégnants et respectés au sein de Nestlé. Rien n'est laissé au hasard. D'autres événements ont heurté des industriels français et d'autres entreprises de l'alimentaire et/ou de l'agroalimentaire en France, cf. Annexe 5.

Conclusion

L'étude réalisée démontre que le terrorisme n'a pas toujours existé, qu'il a parfois été maîtrisé et annihilé. Il reste cependant l'affaire de tous. Bien qu'il s'agisse d'un sujet sensible, c'est par une approche transverse et globale que la lutte contre ce risque est efficace. Le propre du Risk Manager est d'aborder chaque risque en disposant d'un regard assurantiel, il définit ainsi ce qui est assurable ou non. Et l'assurance, quant à elle, permet de couvrir tous types de risques. Or, le risque terroriste ne se saisit pas comme une opportunité. Il est synonyme de danger et aucun bénéfice ne peut en être dégagé pour l'entreprise.

A l'heure de la digitalisation et du Big Data, c'est la mutualisation de l'information entre tous les acteurs de la société qui sera la clef pour déjouer les prochaines attaques. Les Directions Sécurité et Sûreté, les services de Risk Management, les assureurs et courtiers ainsi que les services de l'Etat pourront, ensemble, réduire la menace à néant s'ils parviennent à définir et décliner des plans de maîtrise de risque. Vingt attentats ont été déjoués en France en 2017 – contre 17 en 2016[44]. Qu'en serait-il avec un plan de maîtrise des risques global ?

Enfin, pour le secteur de l'entreprise, les méthodes les plus efficientes pour répondre à une complexification du risque terroriste concernent l'intégration d'audits de sécurité et de sûreté, la vérification systématique de l'identité des collaborateurs et des tiers, la limitation des points d'accès, l'implication des collaborateurs, l'utilisation de stratégies multimodales et la prise en considération des risques psychosociaux. Tous ces procédés sont des applications directes du Risk Management. Appliqués avec l'usage de l'intelligence artificielle, des robots ou encore des nanotechnologies, ils pourraient devenir redoutablement efficaces à long terme.

Comme l'indiquait Denis Kessler de SCOR, « *Le XXIe siècle sera celui du risk management généralisé, ou ne sera pas !* »[45]

[44] Interview du ministre de l'intérieur par le journal *Le Progrès*, 8 janvier 2018.
[45] Denis Kessler (SCOR) interview pour le journal *L'Opinion*, 17 mars 2017.

Bibliographie

Ouvrages, livres et revues

- L'avenir du terrorisme ; Institut Diderot (janvier 2016) – Alain BAUER

- Le terrorisme pour les nuls ; First (juin 2014) – Alain BAUER et Christophe SOULLEZ

- Patron du RAID ; Mareuil Editions (octobre 2017) – Jean-Michel FAUVERGUE & Caroline DE JUGLART

- articles issus des revues : La Tribune de l'assurance, L'Opinion, L'Argus de l'assurance, Atout Risk Manager, Sécurité & Stratégie, Le Point, Le Figaro…

Sites Internet

1) acteursdeleconomie.latribune.fr

2) lesechos.fr

3) rhexpat-avocats.com/fr/prevenir-gerer-risque-terroriste-entreprise/#_ftn14

4) www.lopinion.fr/edition/economie/denis-kessler-scor-xxie-siecle-sera-celui-risk-management-ne-sera-pas-121024

5) www.lexpress.fr

6) www.amrae.fr

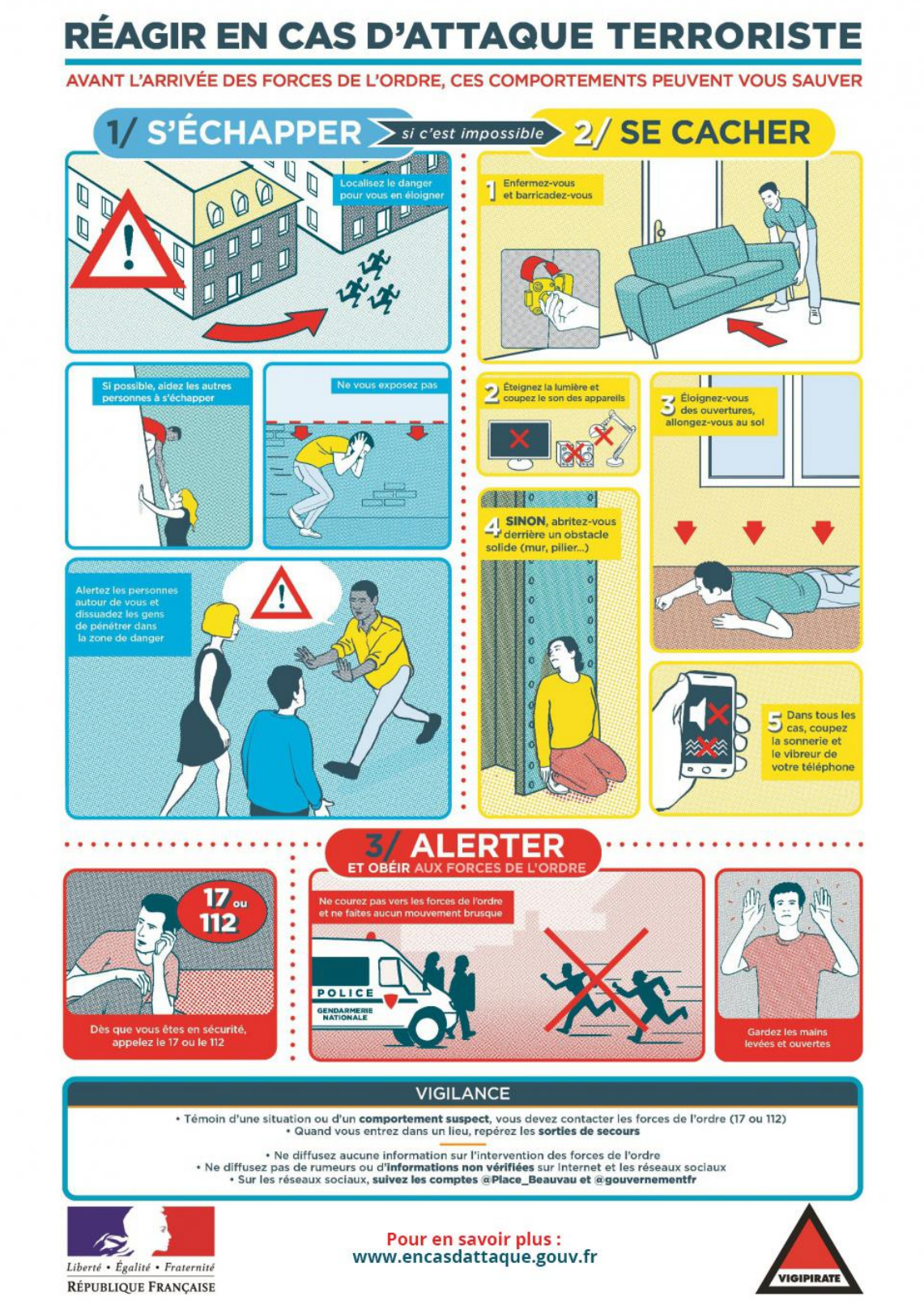
7) stop-djihadisme.gouv.fr

Tables des illustrations

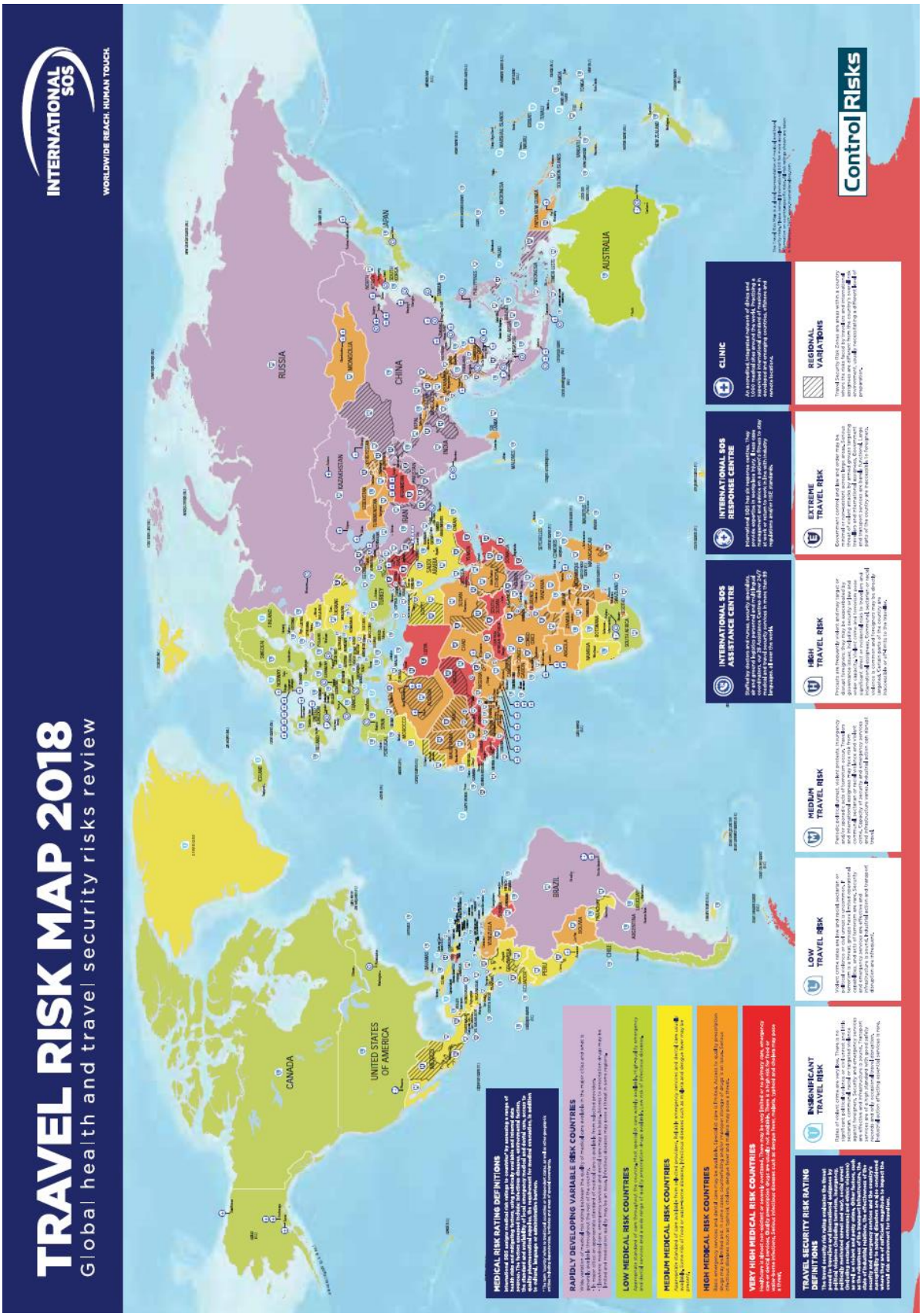
Table des matières

Annexes

ANNEXE 1 : AFFICHE DE SENSIBILISATION AU RISQUE TERRORISTE.



ANNEXE 2 : TRAVEL RISK MAP 2018 PAR INTERNATIONAL SOS



ANNEXE 3 : GRILLE DE SUIVI DES CONTROLES DE SECURITE AU SEIN DES SITES NESTLE FRANCE – A USAGE INTERNE.

GRILLE HEBDOMADAIRE D'EVALUATION SIMPLIFEE POUR LE SUIVI DE LA PRESTATION DE GARDIENNAGE

DATE : **PRESTATAIRE :**

PARTICIPANTS :

DESTINATAIRE : Security Champion USINE et PTC

Bien	100 %
Satisfaisant	90-100 %
Mauvais	80-90 %

Respect des objectifs de la surveillance	
Objectif 1	Assurer la fonction contrôle d'accès– sûreté de l'usine et du PTC
Objectif 2	Assurer la surveillance et les rondes – sûreté de l'usine
Objectif 3	Assurer la surveillance et les rondes – sûreté du PTC
Objectif 4	Garantir la compétence des équipes

Mise en œuvre de la surveillance			
CRITERES	1	2	3
Présentation			
Tenue - courtoisie			
Port des équipements de sécurité			
Formation			
Recyclage à jour			
Nombre d'exercices mensuels	4	3	2
Operations			
Nombre de relèves réussies	5	4	3
RESPECT ET REPORTING DES RONDES			
Accès à la main courante informatisée	5 jours	4 jours	3 jours
TRAITEMENT DES INCIDENTS / ALARMES			
Contrôle d'Agence	4	3	2

Moyenne	Hebdomadaire	Mensuelle	Trimestrielle

ANNEXE 4 : UTILISATION DU BADGE MULTIFONCTION AU SEIN DE NESTLE FRANCE. IMPLANTATION DE CE SYSTEME EN 2014 – DOCUMENTATION A USAGE INTERNE.

ANNEXE 5 : CAS LES PLUS CELEBRES DE CONTAMINATION CRIMINELLE DE PRODUITS ALIMENTAIRES – GUIDE DES RECOMMANDATIONS POUR LA PROTECTION DE LA CHAINE ALIMENTAIRE CONTRE LES RISQUES D'ACTIONS MALVEILLANTES, CRIMINELLES OU TERRORISTES, 2014.

Date	Produits concernés	Type de contamination ou d'agent contaminant	Conséquences	But recherché	Observations
1972		40 kg de culture de Salmonella Typhimurium	Aucune : action préventive de la Police.		2 membres de l'« Ordre du Soleil Levant » arrêtés au Japon en possession des produits
1977	Agrumes en provenance d'Israël	Mercure, vraisemblablement injecté par seringue	• Environ 12 personnes contaminées • Forte chute des exportations d'Israël	Nuire à l'économie d'Israël	
Années 1980	Boissons et divers aliments en Irak	Thallium	Plusieurs dissidents intoxiqués	Elimination d'opposants politiques	
Sept/oct. 1984	Salades (10 restaurants d'une même chaîne) Oregon (Etats-Unis)	Culture liquide de Salmonella Typhimurium	Environ 600 personnes intoxiquées	Une secte religieuse tentait d'influer sur une élection locale	
1989	Raisins chiliens importés aux Etats-Unis	Cyanure	• Aucune personne contaminée • Plusieurs pays ont suspendu leurs importations de fruits du Chili	Nuire à l'économie du Chili	
1991	Eau de Perrier	Traces de benzène dans plusieurs bouteilles	• Rappel des produits • Chute de C.A. : 35%	But et auteurs inconnus	Contamination accidentelle ou non ?
1992	Réservoirs d'eau d'un camp militaire turc à Istanbul	Concentrations létales de cyanure de potassium	Officiellement, aucun militaire contaminé	Empoisonnement de la garnison par le PKK	
1995	Champagne (camp militaire russe au Tadjikistan)	Cyanure	Environ 10 militaires russes morts	Vengeance d'Afghans ? Départ de l'armée russe du pays ?	
29/10/96	Pâtisseries (salle de repos du personnel d'un laboratoire d'un centre médical américain)	Shigella Dysenteriae (provenant des cultures du labo)	12 personnes contaminées, dont 4 hospitalisées (sur un effectif total de 45)	Malveillance	
1996	Divers aliments de divers groupes agroalimentaires en RFA	Venin de serpent (cobras et vipères)	• Renforcement des contrôles • Cellules de crise	Extorsion de 400 M DM en diamants par un mystérieux commando « Tamara S »	Affaire jamais élucidée
Début 2003	Lait de soja dans 8 écoles primaires au Nord de la Chine	Non révélé	• 3 enfants morts • Plus de 3000 intoxiqués	« empoisonnement criminel », sans plus de précision	
Juillet 2004	Boissons, chocolats et fromages de 6 groupes industriels en France	Non déterminé		Tentative d'extorsion de fonds par un mystérieux « groupe AZF » (cas dit « AZF 2 »)	• Affaire toujours en cours fin 2005 • 2 groupes de cosmétiques aussi concernés

ANNEXE 6 : LA PROTECTION D'UN SITE « NBCR », L'EXEMPLE D'EDF.