Malveillance ordinaire dans les installations industrielles

L'événement de l'été 2015 à Saint-Quentin-Fallavier en est une terrible illustration : les installations industrielles peuvent être utilisées comme des armes. Cependant, la malveillance ciblant le monde industriel ne prend pas uniquement la forme d'actes de terrorisme. De nombreux accidents trouvent leur origine dans une autre forme de malveillance, qualifiable d'« ordinaire », mais dont les conséquences peuvent être considérables.

En raison des biens et produits qu'ils manipulent ou des nuisances qu'ils génèrent, les sites industriels ont toujours été des cibles de choix pour les personnes mal intentionnées. Globalement, pas moins de 4 % des accidents survenus dans des installations industrielles françaises depuis 1992 et enregistrés dans la base de données du Barpi (Aria) sont imputés à un acte malveillant avéré ou supposé.

Plus de trois de ces accidents sur quatre (77 %) impliquent un incendie. Outre les cas où la mise à feu volontaire constitue le but premier, les cambriolages se soldent souvent par des incendies lorsque les malfaiteurs cherchent à dissimuler les traces de leur passage. Environ une fois sur deux, il y a pollution de l'environnement. Il s'agit soit de rejets volontaires de matières dangereuses ou polluantes dans le milieu naturel, soit d'émissions de fumées d'incendies. Lorsqu'il y a pollution, les atteintes à l'environnement concernent l'air dans environ 60 % des cas, les eaux superficielles ou souterraines dans 30 % des cas et les sols dans 20 % des cas. Plus de 4 fois sur 5, ces événements ont également des conséquences économiques pour l'entreprise : dommages entraînant des travaux de réparation parfois très lourds, pertes d'exploitation, chômage technique…

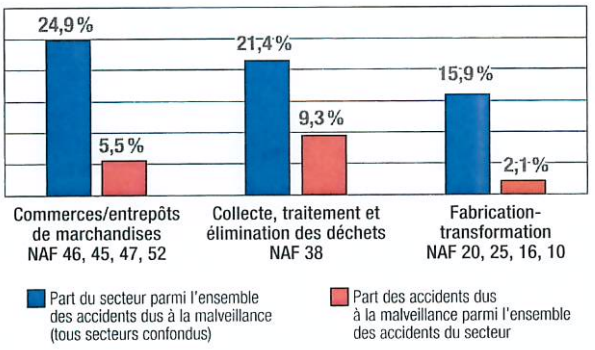
DR

▲ Bouteilles de gaz incendiées dans une station-service.

LES CIBLES PRIVILÉGIÉES DES MALFAITEURS

Les malfaiteurs ont des motivations variées (voir les accidents illustratifs page 11) qui les conduisent à agresser ou à s'introduire dans des installations de divers secteurs d'activités. Les commerces de gros ou de détail (garages automobiles, centres commerciaux, stations-service…) ainsi que les entrepôts de marchandises constituent des cibles privilégiées et représentent un quart des installations attaquées.

En 2e position des cibles favorites se trouvent les installations de collecte et de traitement des déchets. Plus spécialement, les sites possédant des stockages extérieurs ou peu sécurisés : centres de tri, déchetteries, installations de stockage, plateformes de compostage…



De tels sites sont bien plus vulnérables que les centres de traitement des déchets, comme les usines d'incinération, qui bénéficient d'une meilleure sécurisation. Globalement, 9 % des accidents impactant les activités de gestion des déchets sont liés à la malveillance. Bien plus que pour les autres secteurs !

En 3e place sur le podium, avec environ un quart des attaques, se trouvent les installations de fabrication-transformation. Industries chimiques, agroalimentaires et manufactures de produits métalliques sont les plus ciblées de cette catégorie.

VULNÉRABILITÉS RÉVÉLÉES PAR LES ACCIDENTS : DES PISTES POUR ÉVITER LES RÉCIDIVES

Qu'elles soient victimes d'un incendie criminel, d'un cambriolage ou d'un déversement volontaire de substance polluante, les installations industrielles prises pour cibles ont en commun des vulnérabilités dans leurs systèmes de protection. Vulnérabilités dont des personnes mal intentionnées savent tirer profit.

À retenir parmi ces défaillances récurrentes :

• Un entretien des clôtures et un contrôle d'accès insuffisants

De nombreux sites souffrent de clôtures en mauvais état, voire totalement absentes. Parfois, la clôture est présente mais de mauvaises pratiques d'exploitation empêchent le fonctionnement normal des dispositifs anti-intrusion. Par exemple, le positionnement d'équipements le long de la clôture peut neutraliser le fonctionnement du faisceau des cellules anti-intrusion. Plusieurs accidents révèlent ainsi des défaillances criantes au niveau du contrôle d'accès, rendant possible une intrusion dans des locaux renfermant des produits dangereux.

• L'absence de surveillance des sites en période « hors activité »

Les intrus choisissent souvent la nuit, les périodes de fermeture ou d'arrêt temporaire des installations pour s'y introduire. L'absence de gardiennage ou d'autre mode de surveillance pendant ces phases est une erreur courante, en particulier dans le secteur de la gestion des déchets.

• Les sites fermés non mis en sécurité

Les sites désaffectés, abandonnés après une liquidation ou une cessation d'activité sont des cibles de choix pour les pilleurs. En effet, des produits ou marchandises de valeur sont parfois maintenus en place après l'arrêt complet de l'exploitation. L'absence de surveillance et de mesures de protection contre l'intrusion laisse la voie libre aux personnes mal intentionnées. Une configuration rencontrée dans l'ensemble des secteurs d'activités.

• Des équipements vulnérables mal protégés

Les exploitants négligent parfois la protection ➜

DES MOYENS D'ACTION ET TRACES DE PASSAGE RECONNAISSABLES

En fonction de l'installation ciblée et de la motivation des malfaiteurs, les moyens employés diffèrent. S'ils restent généralement simples, ils se révèlent fort « efficaces ». Quelques exemples :

> projection d'une voiture bélier contre un entrepôt de marchandises pour le cambrioler ;

> jet de cocktail molotov dans une installation de stockage pour y déclencher un incendie ;

> ouverture des vannes d'une cuve de stockage de produits chimiques pour initier une pollution ;

> inflammation de bouteilles de gaz dans une station-service.

Ces méthodes laissent derrière elles des indices et traces fort utiles au moment de l'enquête (portails fracturés, clôtures découpées, objets incendiaires tels que des bidons d'essence vides laissés sur place…). Des éléments tels que la présence de foyers d'incendie multiples et simultanés ou encore la découverte d'une réserve d'eau incendie préalablement vidée permettent également d'exclure une origine accidentelle.

Dreal Rhône-Alpes

▲ Grillage découpé par des intrus.

À CHAQUE ATTAQUE MALVEILLANTE, SA MOTIVATION

La malveillance est souvent la manifestation d'une violence « gratuite » par pure volonté de nuire. Cependant, selon sa spécialisation, chaque installation industrielle attire également des malfaiteurs aux motivations bien particulières. Petit tour d'horizon illustré des cas les plus courants.

Objectif Dérober des matières ou objets à valeur commerciale

Métaux, hydrocarbures, denrées diverses… tous les produits à valeur commerciale sont convoités. Dans l'industrie chimique, certaines substances aux propriétés particulières (par exemple substances explosives) attirent également les malfaiteurs.

22 décembre 2005, Heudebouville (Eure)
Un groupe armé, composé de deux hommes et une femme, vole 1 280 kg de poudre d'aluminium dans une usine de fabrication d'encres métalliques pour emballages après avoir neutralisé le gardien de l'entreprise. La police diligente une enquête.

Objectif Manifester un mécontentement dans le cadre de problèmes d'acceptation locale

Une situation rencontrée fréquemment dans le secteur des déchets, dont les installations peuvent engendrer des nuisances pour le voisinage (nuisances visuelles, olfactives, sanitaires…). Mais des cas sont également rencontrés dans d'autres secteurs d'activités.

22 juillet 2001, Turny (Yonne)
Dans une scierie, un tuyau d'alimentation d'un groupe électrogène est entaillé à la sortie d'une cuve de fioul. Les 3 000 l de fioul contenus dans la citerne se répandent sur le site et dans un fossé voisin. L'exploitant répand de la sciure pour absorber le produit. Les pompiers installent un barrage de paille pour éviter que le fioul n'atteigne un cours d'eau. Plusieurs autres actes de malveillance avaient été commis dans le mois précédent. Des problèmes de relations avec le voisinage en seraient à l'origine. L'exploitant va déménager son activité sur un autre site.

> Indices accidents

Matières dangereuses relâchées · Conséquences humaines et sociales · Conséquences environnementales · Conséquences économiques

Objectif Se débarrasser d'objets/produits encombrants ou dangereux

Une problématique plutôt spécifique aux installations de gestion des déchets, exutoires de choix pour des dépôts en tout genre.

22 septembre 2010, Nice (Alpes-Maritimes)
En utilisant une pelle mécanique, un agent d'une déchetterie provoque l'explosion d'un détonateur abandonné dans les encombrants. Les démineurs de la sécurité civile en récupèrent 169 autres et les détruisent dans une carrière proche.

Objectif Manifester dans le cadre de conflits sociaux personnels (désaccord employé-employeur, vengeance post-licenciement…) ou collectifs (grèves, manifestations)

21 janvier 2010, Miserey-Salines (Doubs)
Un salarié en conflit avec son employeur s'introduit vers 21 h 30 dans son entreprise de traitement de surfaces, détériore des machines, met le feu à des cartons et des palettes avant de voler un véhicule. L'incendie est éteint par les secours publics.

17 juillet 2000, Givet (Ardennes)
À la suite d'un conflit social avec leur employeur pour cause de liquidation judiciaire, 153 salariés licenciés, qui occupent une filature de viscose, déversent 5 000 l d'acide sulfurique et des colorants dans un ruisseau traversant l'usine et se déversant dans la Meuse. Les pompiers parviennent à contenir la pollution avant qu'elle n'atteigne la rivière. Un protocole de fin de conflit est signé le 21 juillet.

DR

◀ Pollution volontaire d'un cours d'eau lors d'un conflit social.

Des actes malveillants peuvent aussi avoir lieu dans le cadre d'une crise sociale de grande ampleur sans lien direct avec l'installation industrielle ciblée. Par exemple, des accidents sont survenus dans le contexte des violences urbaines généralisées à Villiers-le-Bel en 2007.

Pour en savoir plus, consultez la synthèse « Accidentologie sur les actes de malveillance dans les installations industrielles » élaborée sur la base de l'analyse de 850 accidents et disponible sur le site Internet Aria dans la rubrique « Synthèses par thème ».

d'équipements ou de matières vulnérables. Premier exemple : celui des stockages en extérieur. Que ce soit dans le secteur des déchets ou dans les activités de production/commerce, ces stockages sans protection bâtie sont fréquemment pris pour cible. La problématique est identique pour les stockages situés en limite de propriété, à proximité des murs d'enceinte, qui peuvent ainsi être approchés sans attirer l'attention.
Globalement, se pose la question de l'implantation géographique des installations. Isolées en rase campagne, elles peuvent parfois être attaquées sans attirer l'attention. C'est également le cas des sites très étendus et donc difficiles à surveiller et à clôturer intégralement. Mais, même dans des endroits *a priori* très fréquentés, certaines zones souffrent parfois d'une surveillance insuffisante. Ainsi, réserves et stocks des supermarchés sont souvent la cible de vols.

• Des lanceurs d'alerte et des retours d'expérience insuffisamment pris en compte

De nombreux exemples révèlent une prise en compte insuffisante de certains signes annonciateurs tels que l'occurrence sur une courte période et dans un périmètre restreint de plusieurs incendies similaires. Les leçons des événements passés ne sont pas non plus toujours utilisées à leur juste valeur. Certaines installations connaissent ainsi des récidives d'actes malveillants, alors qu'une vigilance renforcée et la mise en œuvre de certaines mesures correctives auraient probablement permis de les éviter.

À chacune de ces vulnérabilités correspondent des mesures préventives, techniques ou organisationnelles. Leur mise en œuvre doit permettre de progresser vers plus de sûreté pour les installations industrielles. ■

Pauline Arama
Bureau d'analyse des risques
et pollutions industriels
Ministère de l'Écologie, du Développement
durable et de l'Énergie

La difficile analyse des risques de malveillance

Si les récentes attaques terroristes ont poussé les entreprises industrielles à prendre en compte les risques liés à la malveillance, ces dernières ne savent toujours pas par quel bout les prendre. Très différente de la sécurité, la sûreté demande une analyse bien particulière.

Romain Beurrier-REA

▲ **Incendie criminel à l'usine pétrochimique LyondellBasell de Berre-l'Étang le 14 juillet 2015.**

2015 a été placée sous le signe des actes terroristes. Des actes ont touché une usine en Isère au mois de juin et ont ainsi rappelé aux entreprises leur vulnérabilité face à la malveillance. Car si la sécurité est depuis longtemps prise en compte au sein des entreprises, la sûreté fait bien souvent figure de cinquième roue du carrosse : très peu de sociétés réalisent une analyse de leurs risques liés à la malveillance. Pourtant, d'après une étude du Barpi (Bureau d'analyse des risques et des pollutions), ces risques représentent 4 % des risques industriels c'est-à-dire 68 sinistres par an soit plus d'un par semaine (lire aussi notre article page 9) !

L'État s'est emparé de cette problématique. Au mois de juillet, Ségolène Royal, ministre du Développement durable, a réuni des exploitants de sites Seveso afin de

définir des moyens de lutte contre ce type de risque. Il a notamment été décidé la réalisation d'inspections sur les sites Seveso et une auto-évaluation de leur sûreté. Si le sujet semble au cœur des préoccupations gouvernementales, les entreprises, quant à elles, se sentent démunies face à la démarche à entreprendre. Et ce, dès la première étape : l'analyse des risques.

DES RISQUES DIFFICILES À CERNER

Pourquoi cette analyse des risques est-elle si difficile à mener ? Peut-être parce qu'il s'agit de risques difficiles à cerner. Tout, au sein des industries, peut être une cible : les produits chimiques bien sûr mais aussi de simples robinets, pour le laiton qu'ils contiennent, ou encore des câbles pour leur cuivre, les employés peuvent être agressés, un bâtiment dégradé… Il est difficile de savoir quelle entreprise peut ou non attirer des actes malveillants. Et surtout ce qui peut être visé au sein même de l'entreprise.

Par ailleurs, n'importe quel moyen est susceptible d'être utilisé : voitures béliers, feu, armes, explosifs… La liste est là encore très longue. Sans parler des cyberattaques : il est désormais possible d'attaquer à distance, 24 heures/24 et 7 jours/7. « *La délinquance évolue et les entreprises doivent suivre. Mais elles n'en ont pas toujours les moyens* », observe Gilles Goubin, responsable du Pôle malveillance au département formation de CNPP.

Les entreprises n'ont pas toujours les compétences en interne pour pouvoir réaliser ces analyses de risques. Ces compétences sont en général présentes pour les risques clients/produits (au niveau du responsable qualité), pour les risques sécurité (avec une pratique de près de 15 ans d'élaboration des évaluations des risques professionnels) et pour les risques environnementaux (avec des pratiques anciennes résultant de la réalisation des études des dangers et des études d'impact dans le cadre de la réglementation ICPE). Mais, en matière de sûreté-malveillance, peu d'entreprises ont une expérience et une pratique, voire des compétences internes.

ABSENCE DE NORME

Autre difficulté : il n'existe pas de normes auxquelles se référer. Pour les autres risques il existe des référentiels ISO qui cadrent les démarches d'analyse de risque et fournissent des modèles d'organisation. Pour la sûreté, il existe des normes par secteurs : ISO 27001 pour le management de la sécurité des systèmes d'information, ISO 28000 pour la chaîne logistique… Toutefois, il n'y a pas de norme d'ensemble. Une norme sur le management de la sûreté devrait voir le jour : l'ISO 34001, mais elle est toujours en projet… depuis 2013.

Certains organismes ont essayé de combler ce vide. Comme CNPP qui a développé le référentiel 1302 (Système de management de la sûreté). Le Secrétariat général de la défense et de la sécurité nationale (SGDSN) a mandaté l'Ineris (Institut national de l'environnement industriel et des risques) pour élaborer un guide (voir encadré ci-dessous) afin d'aider les opérateurs de l'industrie chimique à se protéger des menaces de malveillance et du terrorisme. C'est d'ailleurs à partir du questionnaire de cet ouvrage que les installations Seveso doivent réaliser leur auto-évaluation.

ATTRACTIVITÉ ET FACILITÉ

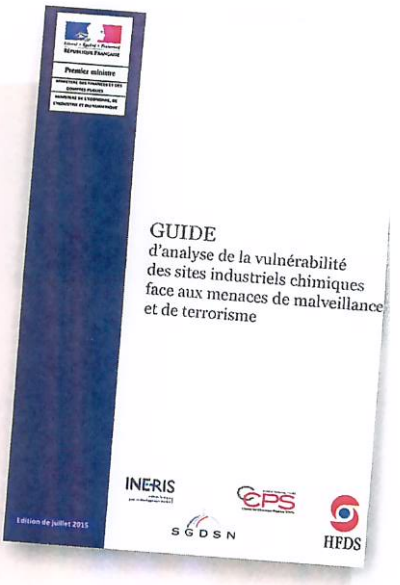
Le guide de l'Ineris présente l'avantage d'offrir une méthodologie adaptée aux actes de malveillance. « *Dans l'analyse classique, les risques sont en rapport avec la fréquence et la gravité. C'est un modèle qui s'applique bien à des événements à fréquence élevée et moyenne mais qui n'est pas adapté au terrorisme, par exemple. Le guide de l'Ineris remplace la fréquence et la gravité par l'attractivité et la facilité* », souligne Olivier Edieu, consultant sûreté à CNPP.

Un référentiel effectivement intéressant mais qui, selon Gilles Goubin, n'est pas facile à appréhender : « *Comment évaluer l'attractivité de son entreprise pour les terroristes ? La probabilité d'une attaque n'est pas facile à définir* ». Le référentiel 6011 (Analyse de vulnérabilité) - CNPP Éditions - qui est une approche globale pour l'incendie ou la malveillance, propose d'analyser son environnement, les cibles de l'entreprise… Afin de les sécuriser.

Lors de la table ronde organisée par *Face au Risque* le 8 décembre 2015 à Mulhouse sur le thème de « L'industrie face à la malveillance », Olivier Edieu a présenté les trois côtés du triangle de la menace : méthodes et moyens d'actions, agresseur, objectif (voir

LE GUIDE DE L'INERIS

Inspiré du « Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites » du Center for Chemical Process Safety (août 2002), le document publié par l'Ineris offre aux industries un questionnaire d'auto-analyse et une démarche d'analyse. Son approche part du même principe que les études de dangers : elle analyse la situation des entreprises via une matrice vraisemblance/gravité. Il s'agit ensuite de faire en sorte de retrouver un niveau acceptable.
L'UIC (l'Union des industries chimiques) s'est attelée à simplifier le questionnaire et devrait bientôt décomplexifier la démarche d'analyse.



Frilled Dragon/Fotolia.com

▲ **Le retour d'expérience permet d'identifier les cibles possibles et les failles de sécurité afin de définir la protection à mettre en place.**

notre article sur les attentats page 18). « *Il faut agir sur l'objectif en durcissant les moyens d'accès à la cible et en recueillant des informations sur l'actualité de la menace.* » Pour ce faire, Gilles Goubin conseille de se référer à des organismes et des associations comme l'Observatoire national de la délinquance, qui délivre une cartographie de la délinquance, ou encore aux chiffres issus d'organismes sectoriels, qui sont plus précis. On peut également faire appel aux statistiques des assureurs. « *Il faut ensuite confronter ces chiffres à la réalité terrain, au ressenti* », insiste-t-il.

S'ATTAQUER AUX PETITS VOLS

Le retour d'expérience est en effet nécessaire afin d'identifier les cibles possibles et les failles de sécurité afin de définir les stratégies de dissuasion et de protection à mettre en place. C'est l'un des avantages du guide Ineris : « *Il propose non pas de partir de la menace et de mettre les mesures en face mais de faire un état des lieux et d'améliorer l'existant* », rapporte Olivier Edieu. « *Il s'agit de s'assurer que l'accès au site est sécurisé : badges, caméras, rondes, clôtures tout le long du site et d'une hauteur suffisante…* », poursuit Gaëlle Dussin, experte en sécurité industrielle au sein de l'Union des industries chimiques (UIC). *Il faut également se soucier des informations disponibles sur Internet.* »

Surtout, une analyse de l'existant permet de mettre à jour les actes de malveillance auxquels l'entreprise est réellement confrontée. Comme les petits vols, sur lesquels les chefs d'entreprise ferment bien souvent les yeux. « *Si des gens sont capables de sortir de petits outillages, cela veut dire qu'il y a une brèche dans la sécurité de l'entreprise et qu'il est possible de commettre des actes plus graves* », pense Olivier Edieu. Il fait référence à la pyramide de l'agresseur : s'il y a effectivement le terroriste à son sommet, sa base est constituée de tout le monde. Tous les salariés peuvent commettre de petits vols si on les laisse faire. « *Il faut faire en sorte que ce ne soit plus possible de voler ou que ce ne soit en tout cas plus attractif* », insiste-t-il.

Il conseille par exemple d'utiliser des technologies type RFID qui permettent de réaliser un inventaire quotidien. Il avertit également du danger de permettre aux véhicules de se garer au sein de l'enceinte : en stationnant près des issues de secours, il est possible de charger facilement des produits dans le coffre. Sans parler du fait qu'on ne sait pas ce qu'il y a dans le véhicule et qu'il est difficile de contrôler l'identité de tous les passagers…

LA VALEUR AJOUTÉE DE LA SÛRETÉ

Ce ne sont donc pas forcément d'importantes mesures qui doivent être prises. « *Le terrorisme est fort en conséquence mais faible en fréquence : est-il vraiment judicieux de mettre en place des moyens lourds qui empêcheraient de poursuivre son activité ? Il faut accepter certains risques* », analyse Gilles Goubin. D'autant plus qu'investir dans la sûreté peut rapidement être onéreux : une clôture coûte par exemple entre 150 et 200 euros le mètre linéaire.

Et est-ce vraiment efficace ? La direction générale peut exiger une garantie que l'argent investi est correctement employé. D'où la nécessité d'aller plus loin qu'une simple analyse des risques basiques. Pourquoi ne pas mettre en place des indicateurs, proposer un programme de formation pour sensibiliser le management à la question de la sûreté… Et surtout démontrer les bienfaits d'une politique sûreté efficace : financièrement mais aussi sur des questions environnementales (49 % des actes de malveillance en entreprise provoquent un rejet de matières dangereuses/polluantes) ou encore sur la question de l'image. ■

Ève Mennesson

Le danger vient aussi du numérique

Alors que le numérique a conquis tous les territoires et s'impose au bureau, à la maison, à l'usine, les attaques de Sony Pictures et le piratage de TV5 Monde rappellent que la menace est également virtuelle.

L'année s'est ouverte par la révélation d'un immense piratage dans les colonnes du *Washington Post* le 5 janvier 2016. Le quotidien y révélait que deux semaines auparavant, à la veille de Noël, l'Ukraine avait été la cible d'une équipe de hackeurs, probablement russes, baptisée SandWorn. Cette équipe, active depuis 2009, a déjà un beau palmarès qui laisse penser qu'elle pourrait être l'émulation d'un État. Elle a ainsi espionné l'ONU en 2013, attaqué un opérateur télécom français et espionné le Gouvernement ukrainien en 2014 jusqu'à ce coup d'éclat de décembre. Elle s'était fait une spécialité de l'attaque des Scada (*Supervisory Control and Data Acquisition*), des automates industriels en quelque sorte. Une spécialité qu'elle a pu particulièrement exploiter lors de cette attaque ukrainienne qui a causé pendant plusieurs heures une coupure de courant dans la région de Kiev et à l'ouest du pays. Pour ceux qui ont analysé l'incident, comme le cabinet américain iSight qui suit le groupe de hackeurs, c'est l'une des premières fois qu'un logiciel malveillant s'attaquant à un automate industriel a un impact sur la vie de dizaine de milliers de personnes. Et pour beaucoup ce n'est qu'un début.

CARACTÉRISTIQUES DE L'ATTAQUE DE TV5 MONDE

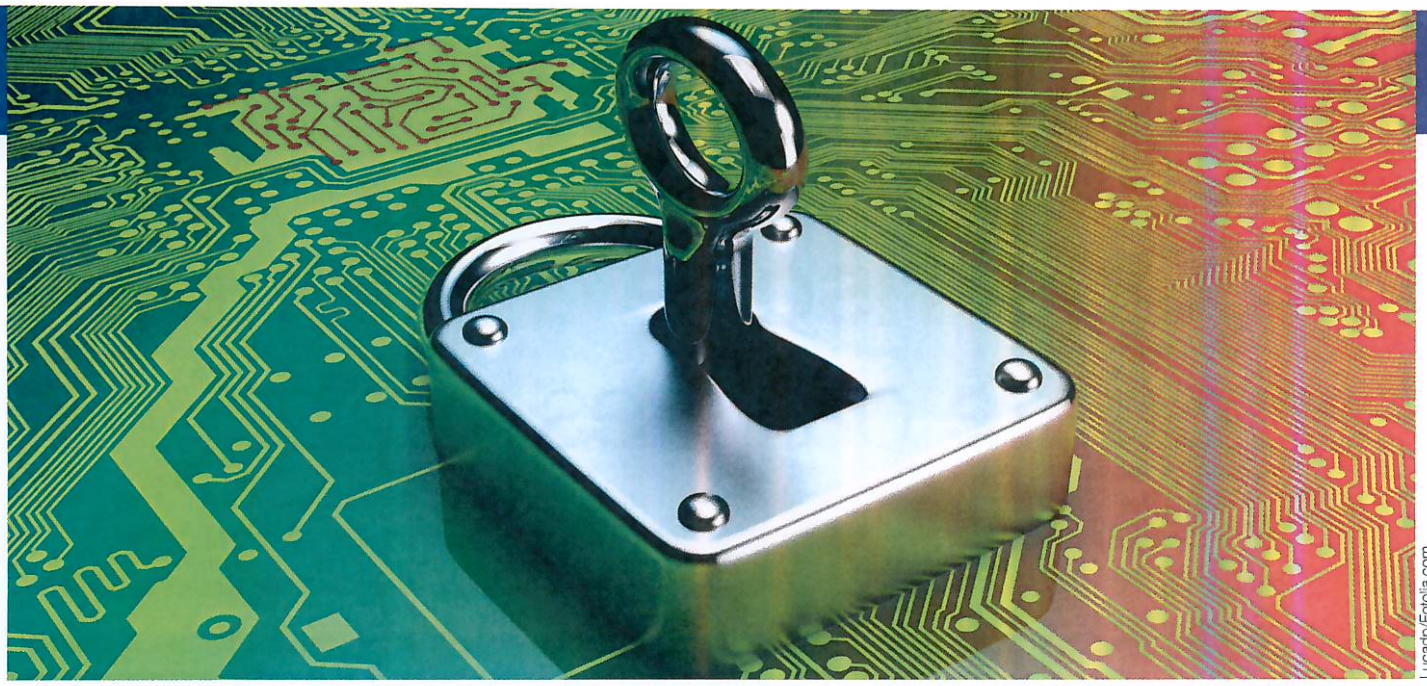
> Attaquants : spécialistes d'origine étatique ou bénéficiant de l'appui et de la protection d'un pays
> Cible : connue et exposée, médiatique (effet maximum), symbolique (voix de la France dans le monde)
> Motivations : représailles ou attaques suite à la diffusion de reportages
> Méthode : attaque longue et complexe nécessitant la coordination de plusieurs acteurs (équipe)
> Moyens : nécessite des équipements multiples, puissance de calcul, renseignement et repérage, exploitation d'une vulnérabilité humaine (mot de passe peu sécurisé)

UN MONDE HYPER CONNECTÉ

Les réseaux et l'informatique ont une telle emprise sur la manière dont le monde, les objets et les hommes sont organisés que le moindre accro peut avoir d'immenses répercussions.
Quel est l'objet qui n'est pas piratable aujourd'hui ? Tout ou presque est connecté : les raquettes de tennis, les réfrigérateurs, les avions, les compteurs, les montres, les hôpitaux, les stations spatiales, les pots de fleurs… Et pour chaque connexion, une vulnérabilité attend d'être exploitée. Ce n'est d'ailleurs pas nécessairement sur le logiciel (software) ou sur le matériel (hardware) que les efforts de l'attaque seront portés, mais plus sûrement sur l'humain, car il reste la pièce la plus vulnérable de l'équation.

TV5 MONDE : LA TECHNIQUE DE CONTRÔLE DU RÉSEAU

Prenons le piratage de TV5 Monde (5 M€), les spécialistes de l'Agence nationale pour la sécurité de systèmes d'information (Anssi) ont pu remonter le fil jusqu'à la vulnérabilité originelle. Fin avril 2015, les enquêteurs ont partagé avec des grands médias nationaux quelques-unes des preuves accumulées. La piste du mystérieux « Cyber caliphat » lié à l'État islamique s'est éloignée et des indices ont conduit à un groupe russe baptisé « Pawn Storm » (tempête de pions) par les analystes de Trend Micro. Le mode opératoire a été soigneusement étudié et livré dans les colonnes du *Monde* au mois de juin 2015 : les pirates ont d'abord investi un ordinateur d'un poste de production « *servant à contrôler les caméras sur le plateau* ». Ce dernier, qui servait à un prestataire du groupe, disposait d'un mot de passe peu sécurisé qui a pu être facilement cracké. La suite a été possible grâce à une absence d'étanchéité entre les réseaux de production de la télévision et la partie administrative de la chaîne publique. Pendant plusieurs semaines, le groupe a ainsi pu



Lucadp/Fotolia.com

▲ Les attaques numériques sont désormais orchestrées par les grandes puissances qui s'affrontent. Les entreprises doivent renforcer leur protection face à des structures très organisées qui peuvent aussi les atteindre par ricochets.

évoluer dans le système informatique et patiemment se lancer à la conquête de droits d'accès. Une technique qu'on appelle « l'élévation de privilèges ». Il s'agit d'obtenir les droits d'administration du système, même de manière temporaire, pour contrôler l'intégralité du réseau. Une fois ces droits acquis, le groupe est passé à l'offensive qui s'est matérialisée par la destruction physique de matériels. Pour beaucoup, cette attaque est une attaque contre un média pour l'empêcher de diffuser des nouvelles. Or il s'agit d'une erreur d'analyse. Certes, il y a eu volonté de stopper la diffusion mais, à cette volonté, s'est ajoutée celle de détruire du matériel de manière irréversible. En cela, cette attaque est dirigée contre l'outil de production.

Les attaques numériques du milieu des années 2010 ne sont plus des attaques symboliques où l'on cherche à gagner en visibilité mais davantage des attaques étudiées et réalisées par des spécialistes qui veulent détruire et impacter des entreprises ou des États. Qu'il s'agisse de Sony Pictures ou de TV5 Monde, ces attaques retentissantes avaient avant tout des visées politiques.

UNE GUERRE D'ÉTATS

Les États-Unis et Israël ont ouvert le bal au début de cette décennie avec le ver Stuxnet qui a détruit des centrifugeuses à Natanz (Iran). En 2012, le ver Shamoon s'est attaqué aux alliés américains en détruisant des ordinateurs et en paralysant le service d'installation gazière au Qatar. On pourrait multiplier les exemples de ces attaques/ripostes entre les États-Unis, la Chine, la Russie, le Moyen-Orient, l'Europe… Ces premiers éléments montrent que le jeu numérique est désormais un jeu de puissance, un jeu géopolitique où les grandes puissances s'affrontent. Ce n'est plus le fait de hackeurs désocialisés qui passent leurs nuits à coder dans le garage de leurs parents mais bien plus des équipes organisées bénéficiant d'un soutien technique et logistique, appliquant des méthodes élaborées pour parvenir à leur fin.

La bonne nouvelle, c'est que l'attaque n'est pas à la portée du premier venu. Cela signifie aussi que les entreprises doivent considérablement renforcer leur protection face à des structures extrêmement bien organisées et qui peuvent frapper par ricochets ou les atteindre comme dommages collatéraux. À l'époque de Stuxnet, plusieurs entreprises occidentales ont eu des sueurs froides avec des incidents liés à ce ver dont elles n'étaient pas la cible et qui ne devaient pas les atteindre.

LES ENTREPRISES DOIVENT ANALYSER CES RISQUES

La prise de conscience est progressive. Fin 2012, l'Anssi a mis en ligne un guide pour la maîtrise de la sécurité des systèmes d'information pour les systèmes industriels. Mais, dans l'industrie, le chemin est encore long. Lors d'une présentation fin septembre 2015, le cabinet Lexsi précisait que lors, de leurs audits, plusieurs clients n'avaient pas conscience de leur vulnérabilité : « *L'usage et la facilité l'emportent souvent sur la sécurité. On a ainsi découvert qu'un opérateur avait installé un système de prise en main à distance sur un système de contrôle commande, ce qui lui permettait parfois de contrôler que tout se passait bien depuis chez lui. Sauf que cette porte permettait littéralement d'atteindre l'ensemble du système de l'entreprise.* »

Pour compléter le guide de l'Anssi, les éditions Cépaduès proposent un ouvrage collectif « Cybersécurité des installations industrielles ». Il s'agit du premier ouvrage complet et en français sur ce sujet. À travers 532 pages, les auteurs détaillent l'historique de la menace et les évolutions qui ont vu le passage des automatismes vers le monde de l'Internet. Comme la sécurité physique, celle-ci doit être conçue en globalité à travers une approche rigoureuse et une analyse précise des risques. Des méthodes, des concepts qui étaient jusqu'à présent inexistants dans des métiers où certes la démarche qualité est connue mais où la préparation aux attaques doit encore progresser. ■

David Kapp

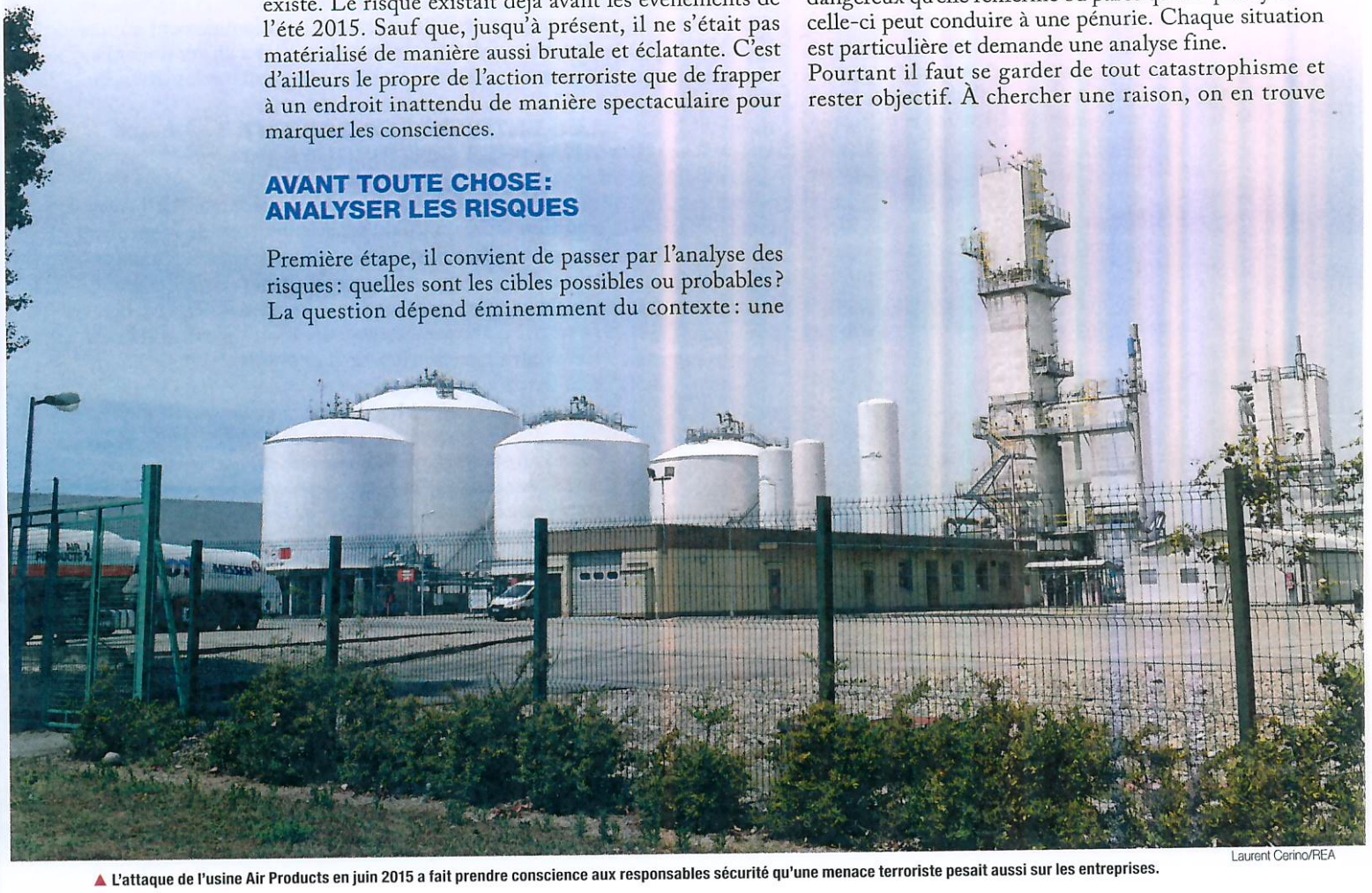
Quel risque d'attentat terroriste dans les usines ?

L'attaque de l'usine Air Products le 26 juin 2015 et les explosions sur le site pétrochimique de LyondellBasell à Berre-L'Étang ont interrogé l'ensemble des responsables sécurité sur la réalité de la menace qui pesait sur leurs organisations. Y a-t-il un risque terroriste pesant sur l'industrie ? De quelle nature ? Comment y faire face ?

Y a-t-il un risque terroriste ? La facilité voudrait que la réponse soit dans la question. Oui, puisque des incidents se sont produits, le risque existe. Le risque existait déjà avant les événements de l'été 2015. Sauf que, jusqu'à présent, il ne s'était pas matérialisé de manière aussi brutale et éclatante. C'est d'ailleurs le propre de l'action terroriste que de frapper à un endroit inattendu de manière spectaculaire pour marquer les consciences.

AVANT TOUTE CHOSE: ANALYSER LES RISQUES

Première étape, il convient de passer par l'analyse des risques : quelles sont les cibles possibles ou probables ? La question dépend éminemment du contexte : une industrie alimentaire peut être ciblée dans une perspective d'empoisonnement tandis qu'une industrie chimique est visée pour les produits potentiellement dangereux qu'elle renferme ou parce qu'une paralysie de celle-ci peut conduire à une pénurie. Chaque situation est particulière et demande une analyse fine.
Pourtant il faut se garder de tout catastrophisme et rester objectif. À chercher une raison, on en trouve



Laurent Cerino/REA

▲ **L'attaque de l'usine Air Products en juin 2015 a fait prendre conscience aux responsables sécurité qu'une menace terroriste pesait aussi sur les entreprises.**

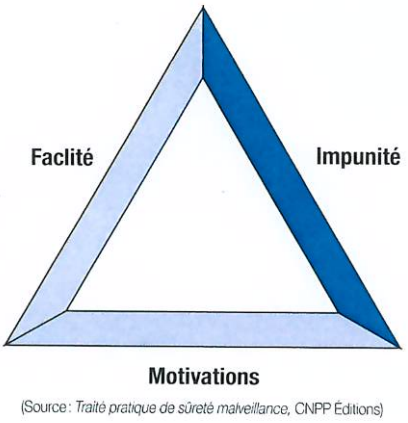
toujours une. L'action terroriste n'est pas toujours froide et calculée. Elle peut aussi être le fait d'une opportunité. Pour chaque attentat, fleurissent des explications, plus ou moins convaincantes sur la symbolique du lieu, de la date et de la méthode utilisée. Or, dans de nombreux cas, c'est bien souvent la facilité ou l'opportunité qui expliquent le choix de la cible. Par exemple, dans l'attaque du centre de soins pour handicapés à San Bernardino aux États-Unis perpétrée par un couple (14 morts), l'un des deux suspects abattus par la police avait travaillé dans ce centre.

Pour analyser les risques, il faut pouvoir élaborer des scénarios probables ou réalistes, là où le terrorisme cherche l'extraordinaire et l'effroyable. Il est important, à ce stade, de se baser sur le retour d'expérience. Celui-ci doit être le plus complet possible. Certaines méthodes d'attaques pratiquées à l'étranger peuvent être transposées plus tard à proximité. Ce fut le cas en novembre avec des attentats suicides qui n'avaient jamais été perpétrés en métropole. Des anciennes attaques peuvent réapparaître à la faveur d'une nouvelle vulnérabilité.

En outre, dans « le feu de l'action », il faut composer avec l'émotion suscitée par les attentats. Des questions sont posées par les représentants du personnel. Des actions doivent être menées. Le propre d'une action terroriste est de surprendre. Si une porte est fermée, l'action se déroulera à la fenêtre. À moins que son auteur choisisse de frapper la maison d'à côté.

Prenons une attaque avec des armes de guerre. Les mesures adoptées pour s'en prémunir sont extrêmement coûteuses et peu rentables : vitrages blindés, agent d'accueil disposant de gilets pare-balles… C'est le moment de profiter des crédits qui pourront être accordés pour passer des mesures peut-être plus anciennes mais qui pourront avoir des retombées immédiates sur d'autres activités. C'est ainsi que l'installation ou le renforcement de clôture aura des effets sur la démarque inconnue… Un sas d'accueil pourra prévenir des braquages, une vitre de sécurité, des incivilités… Tout est affaire de dosage juste.

Le triangle de l'agresseur



(Source : *Traité pratique de sûreté malveillance*, CNPP Éditions)

La démarche de prévention situationnelle s'intéresse à l'agresseur et à ses motivations à agir (voir le triangle de l'agresseur).

On trouve également dans certaines règles techniques des informations sur l'attaquant. C'est le cas dans la norme NF EN 1627 (blocs-portes pour piétons, fenêtre, façades rideaux, grilles et fermetures – résistance à l'effraction de novembre 2011) et le règlement particulier T64 (A2P H64 : Blocs-portes de bâtiment, juillet 2015) qui classent les attaquants en fonction de leurs méthodes et moyens d'actions.

Dangerosité des agresseurs

Dans la pyramide ci-dessus sont représentés les attaquants en fonction de la sophistication de leurs méthodes. Plus on monte dans la pyramide, plus l'attaquant dispose de moyens et de méthodes d'actions. En revanche, plus dispersés et rares sont les candidats à tenter l'aventure. Les frontières ne sont parfois pas si nettes entre les catégories exposées ici et il faut se méfier de toutes les généralisations.

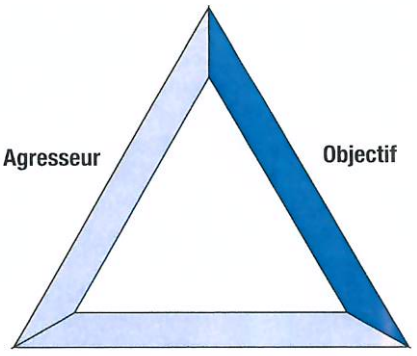
LA MENACE TERRORISTE

La définition même de terroriste pose question car elle est loin de faire l'unanimité. Les organisations internationales s'entendent cependant à définir une action terroriste comme celle visant à contraindre un gouvernement légitime à prendre ou ne pas prendre des décisions.

Dans cette pyramide, la menace terroriste est la plus redoutable : l'individu dispose de moyens conséquents, en général d'un support logistique, il peut également agir avec des complicités, y compris dans des sphères criminelles proches (criminalité de droit commun). Enfin le terroriste peut, dans certains cas, être prêt à mettre sa vie en jeu lors d'une attaque. De ce fait, il est extrêmement difficile à dissuader.

Si on s'intéresse à la menace terroriste et à sa concrétisation imagée ci-après à travers trois facteurs (agresseur, objectif, méthodes et moyens d'actions), on constate que l'entreprise est dépourvue de ressources sur deux facteurs.

Le triangle de la menace



(Source : *Traité pratique de sûreté malveillance*, CNPP Éditions)

Elle a ainsi peu de prises sur l'agresseur qui sera dans la plupart des cas extérieur à l'entreprise. Si la menace provient de l'intérieur, alors ses pouvoirs seront réduits et limités. L'investigation sur les salariés est très limitée et le risque est alors de voir sa responsabilité engagée dans des actions illégales (atteinte à la vie privée, atteinte à la liberté, etc.).

Dans une démocratie, les actions sur l'agresseur (renseignement, interception…) sont un monopole de l'état régalien de même que les actions sur les méthodes et moyens d'actions (le contrôle de l'accès aux armes, par exemple). Le seul champ pour l'entreprise réside dans l'action sur l'objectif.

L'entreprise peut ainsi durcir la cible. Par exemple, s'il s'agit d'un dépôt d'explosifs, elle peut renforcer les protections et les méthodes d'accès aux valeurs. Elle peut également complexifier le cheminement vers les valeurs ou encore retirer toute valeur à la cible. Par exemple, pour les explosifs, on peut multiplier les dépôts et diminuer les quantités stockées ce qui dévalorise l'attaque d'une cible. C'est cette méthode que les banques ont utilisé en diminuant les espèces au guichet pour limiter les braquages. C'est également ainsi que, durant les fêtes de Noël, la Belgique a choisi de protéger ses habitants en interdisant tout rassemblement. En supprimant le gain, on supprime la menace. Il faut noter que cette solution est souvent temporaire et, qu'à un moment ou à un autre de la chaîne, la menace peut réapparaître. Il est alors essentiel de procéder une fois de plus à l'analyse des risques car les gains peuvent beaucoup dépendre du secteur d'activité.

OBJECTIFS D'UNE ATTAQUE TERRORISTE EN INDUSTRIE

Quels peuvent être les objectifs d'une attaque terroriste en industrie ? Les raisons ne manquent pas :

- atteintes aux employés, fournisseurs, clients, public…
- atteintes aux biens ;
- atteinte à l'image (quel est le symbole renvoyé par l'entreprise ?) ;
- vol ou détournement de valeurs ;
- chantage ;
- fraude pour financer une activité ;
- attaque de la population ;
- utilisation des services, utilités, produits, infrastructures de l'entreprise pour commettre une attaque…

Tout dépend du secteur d'activité, de l'actualité de la menace et de la typologie des attaquants. La menace est cependant difficile à prévoir. Par exemple, dans les numéros de *Dabiq* ou *Dar-al islam*, les revues de propagande de Daesh, tout est désigné comme une cible, toute arme peut être utilisée pour frapper.

La menace pour l'industrie ne doit pas non plus être surévaluée car elle est le plus souvent peu rentable dans un cadre terroriste.

L'EXEMPLE DES AÉROPORTS

En 2014, deux chercheurs, l'un Américain, l'autre Australien, se sont très sérieusement penchés sur l'aspect économique de la sécurité des aéroports. Pour

Les cibles des terroristes sont multiples : une industrie alimentaire peut par exemple être visée dans la perspective d'un empoisonnement.

Sanymsakov.com/Fotolia.com

asseoir leur analyse, les chercheurs ont étudié particulièrement l'aéroport international de Los Angeles qui a fait l'actualité le 1er novembre 2013 suite à une fusillade ayant duré en tout 3 minutes et 30 secondes et causé la mort d'une personne. Les problèmes de coordination avec la police avaient alors été soulevés.

Dans un aéroport, la foule est plus clairsemée que dans un stade par exemple, si bien que l'attractivité de la cible pour un terroriste reste encore à démontrer. Des exemples d'actions existent. Sans surprise, écrivent les auteurs, l'approche classique, qui ne prend pas en compte la probabilité d'attaques, trouve toujours très rentable la mise en place de mesures de sécurité. Il s'agit ainsi souvent de mettre en avant les vulnérabilités et de recommander ensuite le renforcement des mesures de sécurité, sans s'intéresser à leur coût ou même parfois à leur efficacité. Cette approche n'est pas celle des deux auteurs qui se sont servis d'une base de données recensant les attaques terroristes sur 40 ans. La probabilité d'une attaque dans un lieu et à un moment donné peut être très élevée en raison du contexte mais elle est très faible au niveau mondial. Si bien que leurs résultats sont différents mais sont aussi plus précis et peuvent être pondérés en fonction du lieu.

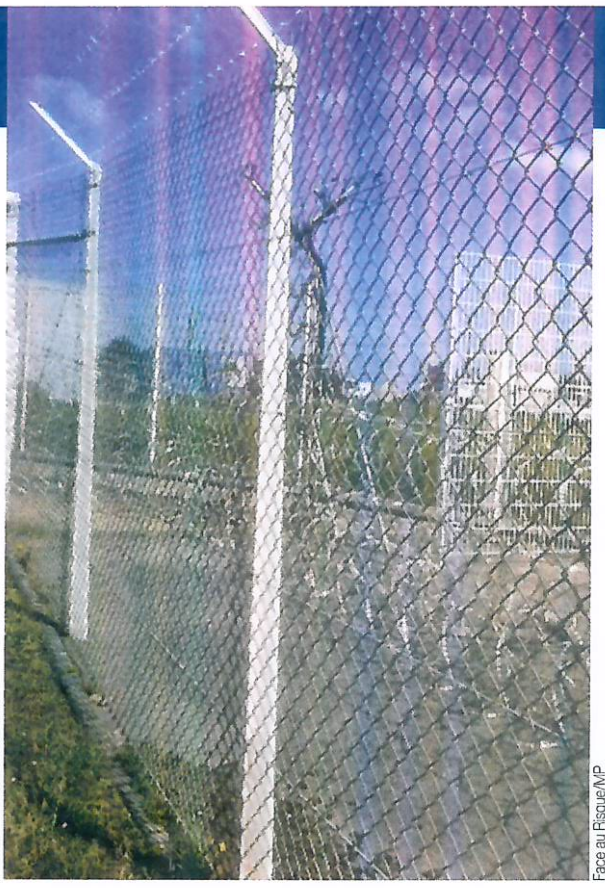
Ainsi, prenons la probabilité de dommages liés à un engin explosif improvisé (IED). Dans les pays occidentaux, la probabilité que ces IED réussissent à faire des dommages dans un aéroport est réduit de 19 % par rapport aux autres pays. Il y a en Occident moins d'opportunité d'acquérir des compétences dans la réalisation de ces engins qu'ailleurs dans le monde.

Et les auteurs tirent la conclusion qu'il faudrait que la probabilité d'attaques soit bien plus importante pour justifier des mesures de protection supplémentaires comme des portiques de détection d'explosifs aux entrées. Et encore, ils admettent avoir surestimé l'efficacité des mesures de sécurité et volontairement occulté le coût indirect lié à de nouvelles mesures telles que la gêne et les inconvénients pour les voyageurs.

L'INDUSTRIE PÉTROCHIMIQUE

Pour l'industrie, c'est un peu la même chose, en particulier l'industrie pétrochimique qui est souvent en tête lorsqu'on parle d'actes de destructions ou d'explosions. Prenons deux événements particulièrement frappants : AZF et plus récemment Tianjin (en Chine), qui ne sont pas des attaques terroristes mais qui peuvent donner une idée de la dévastation que peut causer un acte volontaire.

Événement	Quantité de produit	Conséquences	Pertes humaines
AZF	Entre 120 et 300 t de nitrate d'ammonium	Un cratère ovale de 65 X 45 et de 7 à 10 mètres de profondeur 3,4 sur l'échelle de Richter	32 morts Des milliers de blessés
Tianjin	Plus de 700 t de produits chimiques	Un cratère de 80 m 2,3 et 2,9 sur l'échelle de Richter	173 morts (dont 104 pompiers)



Face au Risque/MP

L'installation ou le renforcement de clôture pour se prémunir d'actes terroristes aura aussi des effets sur la démarque inconnue. ▶

Si ces actions avaient été volontaires, leur « rentabilité » destructrice aurait été faible parce qu'elles demandent non seulement des compétences, du savoir, des repérages mais au final pourraient paraître moins spectaculaires qu'une attaque sur des cibles plus compactes. On pense aux attaques au hasard qui sont traumatisantes et parce qu'elles visent aussi des personnes non protégées. Il est plus facile et plus rapide d'atteindre une cible dans un stade que dans une usine.

L'accident de Tianjin a été particulièrement meurtrier parce que la première explosion a été suivie d'une seconde qui a surpris les secours alors qu'ils arrivaient sur les lieux. Lors du 11 septembre 2001, le lourd bilan humain s'explique aussi par l'arrivée des pompiers sur place pour secourir les victimes (343 pompiers décédés). La méthodologie, une explosion suivie d'une réplique au moment où les secours se rendent sur les lieux, a déjà été employée lors d'attentats en Irak et au Liban. Elle pourrait être transposée.

Bien que l'élément de surprise participe à l'acte de terreur, on peut estimer que, plus vraisemblablement, l'industrie chimique ne présente pas les caractéristiques d'une cible pour un attentat. En revanche, elle pourrait être la cible d'un acte de prédation par des terroristes qui souhaiteraient confectionner une bombe NRBC. Cette prédation pourrait avoir lieu par le biais d'une attaque. Là encore il faut être prudent et analyser la situation sereinement. L'éventail des menaces est large et seulement limité par l'imagination humaine. Et garder en tête qu'une analyse de risque est une manière mathématique de poser un pari sur l'avenir. Pas une garantie. ■

David Kapp