Ne peut être vendu séparément

Spécial

VOYAGES D'AFFAIRES

Supplément de Voyages & Stratégie n° 201

NOVEMBRE - DÉCEMBRE 2018

www.specialvoyages-affaires.com

LOS ANGELES

SOUS LES PALMIERS, LA VILLE

TABLE RONDE

Les programmes entreprises des compagnies aériennes

TRANSPORTS

Affrètement et aviation d'affaires

BUSINESS

La sûreté/sécurité hôtelière

SÛRETÉ/SÉCURITÉ HÔTELIÈRE

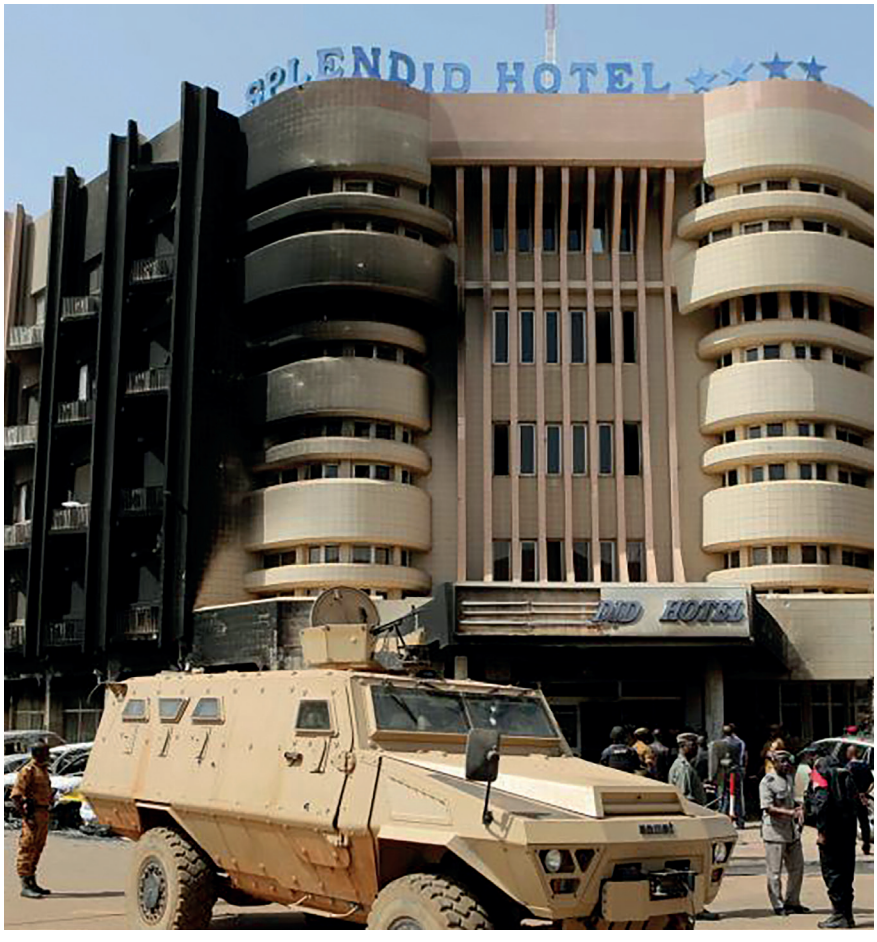
Dormez tranquilles...

Parce que l'hôtel est le lieu de vie principal d'un voyageur d'affaires, sa sélection constitue un élément central d'une politique de voyages sécurisée.

Par David Keller

Chacun le jure la main sur le cœur : cette fois-ci, on a compris. De l'Hôtel Corinthia de Tripoli (2015) à l'InterContinental de Kaboul (janvier 2018) en passant par Tunis, Grand-Bassam, Ouagadougou ou Bamako, la lugubre litanie des attentats perpétrés dans des hôtels ces cinq dernières années aurait finalement accompli son œuvre pédagogique : dans la chaîne du déplacement professionnel, l'hôtel reste bien le maillon faible en matière de sécurité. Une clientèle internationale qui donne de la visibilité à une potentielle action terroriste, un rôle central qui le rend précieux aux yeux du pouvoir en place, une sécurisation moindre que celle dont bénéficie un bâtiment officiel ou un aéroport : tout concourt à renforcer cette vulnérabilité. Et pourtant…

Pourtant, une étude publiée cet été par la société de gestion des risques International SOS et ACTE Global (Association of Corporate Travel Executives) révèle que « *seulement 19 % des entreprises prennent en compte les*



© REUTERS-Joe Penney

paramètres de sûreté et de sécurité dans leur processus de sélection des hôtels ». Une proportion faible mais qui - les professionnels l'assurent à l'unisson - progresse. Selon, la responsable régionale sûreté d'International SOS, Charline Gelin, l'époque où « *les seuls critères de choix d'un hôtel étaient le coût, la localisation et les programmes de fidélité est révolue* » pour un nombre croissant d'entreprises.

Bunker ou low profile ?

Quelques outils commencent à répondre à ce besoin d'information en matière de sécurité. L'OSAC (Overseas Security Advisory Council, rattaché au Département d'État américain) propose un formulaire des performances sûreté/sécurité des hôtels. De ce côté-ci de l'Atlantique, c'est la société Onyx qui promeut sur ces questions le label InSCeHo. Ces efforts de synthèse, de modélisation ou de normalisation sont louables et même d'une grande utilité comme

En haut les abords de l'hôtel Onomo de Bamako; en bas, son ouverture sur l'extérieur se fait dans sa propre enceinte.

©DR


©DR

QUESTIONS À…


©DR

***Ludovic Guerineau**, directeur des opérations d'Anticip. Anticip conseille les entreprises mais aussi les groupes hôteliers dans la gestion des risques en zones sensibles.*

« LA SÉCURITÉ EST AUJOURD'HUI UN VRAI ARGUMENT COMMERCIAL POUR LES HÔTELS »

Quel travail effectuez-vous en direction des hôtels ?

Nous effectuons des préconisations pour la mise en place d'un dispositif sur l'hôtel ayant pour objectif de protéger son bâtiment, ses employés et ses clients. C'est un ensemble de mesures physiques, techniques, et organisationnelles. Il s'agit bien d'un « et », pas d'un « ou » : si un système d'alarmes ou de caméras est mis en place sans qu'une action humaine soit prévue en cas d'alerte, ça ne sert à rien. Et s'il n'y a pas l'organisation pour faire fonctionner tout ça, ça ne marche pas non plus.

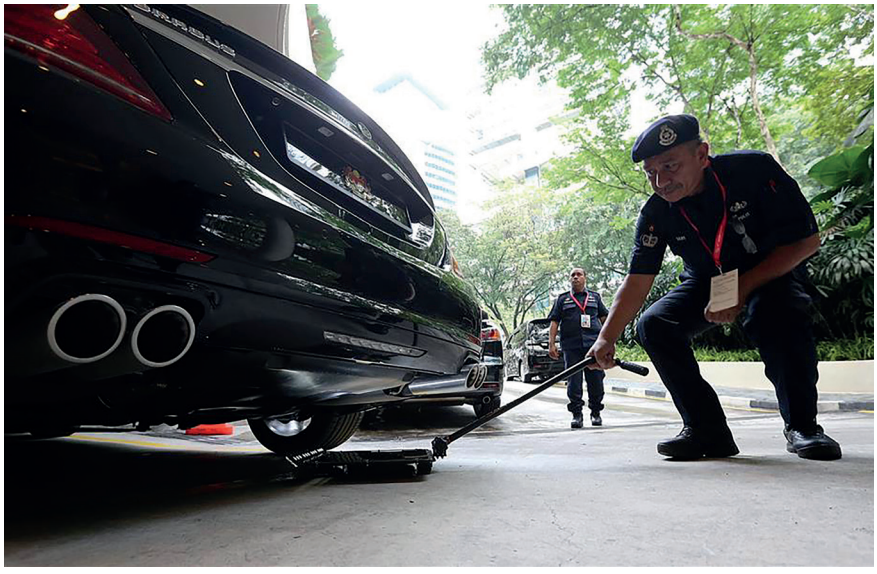
À quels risques les hôtels sont-ils les plus exposés ?

Le risque terroriste est le plus visible, même si les zones où le risque est élevé sont très minoritaires dans le monde. Les autres risques relèvent de la criminalité courante : vol, agression. Là, tous les hôtels du monde sont concernés. C'est une criminalité qui vient soit de l'extérieur de l'hôtel - particulièrement problématique pour les hôtels ayant un accès direct à la rue - soit de la malveillance du personnel. Notons enfin le risque incendie, qui peut d'ailleurs être lié au terrorisme : il y a une tendance récente dans les modes opératoires qui consiste à déclencher un feu pour faire sortir la clientèle de l'établissement et la rendre plus vulnérable.

« Une tendance récente »… C'est donc que les risques évoluent, au moins dans leur forme ?

Oui, il faut procéder à un travail d'évaluation de la situation générale mais aussi à une veille sur les modes opératoires et adapter en permanence la réponse. Mais la situation idéale, tant pour des raisons de fiabilité que de coût, est de penser la sûreté de l'hôtel dès sa conception. Le cas échéant, on peut toujours améliorer le dispositif, quitte à prendre des mesures onéreuses : construction d'un mur d'enceinte surmonté de concertinas (*bobines de fil de fer doté de lames de rasoirs*, N.D.L.R.), installation d'un poste de contrôle à l'entrée avec scanner à bagages, déploiement de chiens détecteurs d'explosifs… Traditionnellement, l'architecture hôtelière est ouverte sur l'extérieur, vitrée. À mesure que les hôtels ont été des cibles, ils se sont repliés sur eux-mêmes. Un de nos clients, l'hôtel Onomo de Bamako, a été conçu sur ce principe. Quand on voit ses photos de l'extérieur, ce n'est pas forcément attirant. Mais c'est un hôtel très sûr, dont l'ouverture se fait à l'intérieur sur un agréable patio. C'est pour ces raisons de sûreté que, lors de son dernier voyage au Mali, Angela Merkel et sa délégation y ont séjourné. Ce n'est pourtant qu'un 3 étoiles. Mais la sûreté est aujourd'hui un vrai sujet pour les clients et, par voie de conséquence, un vrai argument commercial pour les hôtels.

> « Les micros ? Il faut partir du principe qu'il y en a partout. »
>
> ***Charline Gelin***
> *Responsable régionale sûreté d'International SOS*


©Filepic

premiers filtres, mais en plus d'être nombreux et mouvants, les critères de sûreté/sécurité des hôtels sont dépendants de variables qui concernent la localisation bien sûr, mais encore le déroulé du séjour et le profil du voyageur. Un véritable casse-tête qui requiert du sur-mesure.

Car du profil du voyageur découlent des besoins et donc des vulnérabilités différentes. Et selon que l'on est une personnalité publique ou un anonyme, un homme ou une femme, un groupe ou un voyageur isolé, une personne en bonne santé ou sous traitement médical ; le risque diffère. Mais dans cette segmentation du risque, tout commence bien sûr par la localisation. Même si les attentats de Bruxelles ou de Paris ont été conçus pour souligner que personne n'est en sécurité nulle part, il n'en reste pas moins que la potentialité d'un attentat n'est pas la même à Zürich et à Kaboul.

Dès lors, dans le cas d'un risque élevé ou extrême d'attaque terroriste, les dispositifs de sûreté de l'hôtel doivent évidemment faire l'objet d'une très grande attention. Mais selon les modes opératoires observés dans la zone, on pourra préférer un hôtel éloigné de la rue pour éviter les attentats à la voiture piégée ou bien ceux dotés d'une garde armée aux entrées pour éviter les intrusions. Parfois des risques élevés peuvent être très circonscrits dans le temps. Cela peut être le cas, notamment, de troubles sociaux-politiques, qui émergeraient, particulièrement lors d'une campagne électorale par exemple. Dans ce cas, une localisation éloignée de bâtiments officiels qui pourraient être pris pour cibles ou proche de l'aéroport pour une évacuation rapide peut être souhaitable.

« *Globalement,* explique Bernard Jacquemart, directeur de l'Information de Scutum Security First, *le dilemme est de choisir entre des hôtels du quartier business, ultra-sécurisés, bunkerisés mais regroupés dans un quartier cible, ou bien des établissements plus low profile, à la sécu-*

5 RÈGLES DE CYBERSÉCURITÉ

1. Avant le départ : mettre à jour tous les programmes et applis de vos appareils mobiles, anti-virus inclus.
2. Ne pas diffuser en ligne votre localisation exacte ou l'objectif de votre voyage d'affaires.
3. Éviter de vous connecter à des sites non sécurisés (wi-fi public).
4. Déconnecter tous vos appareils des fonctions wi-fi et Bluetooth.
5. Au retour : si votre destination était à haut risque ou que vous avez des doutes, faire vérifier par votre département IT tout signe de logiciel malveillant, accès non autorisés, corruption ou intrusion. Ne connecter vos appareils à des réseaux sensibles qu'une fois la vérification effectuée.

SÉCURITÉ, EST-CE SI SÛR ?

La sécurité consiste à se prémunir contre des risques accidentels : catastrophes naturelles, risques sanitaires…
La sûreté consiste, quant à elle, à se prémunir contre des actes volontaires : terrorisme, criminalité…
La distinction n'est pourtant pas aussi claire dans les faits. D'abord parce qu'il y a souvent interpénétration des 2 notions : un risque élevé d'agression criminelle (sûreté) provoque du stress (sécurité) ; un coup d'État peut contraindre le voyageur à un confinement de plusieurs jours (sûreté), l'obligeant ainsi à se priver de son éventuel traitement médical (sécurité), etc. Le distinguo est d'autant plus délicat que les professionnels eux-mêmes reprennent des formulations hybrides. Ainsi, le terme de « cybersécurité » (et non « cybersûreté »), repris par tout le monde, souligne à tort qu'une action de hacking est imputable à la fatalité plutôt qu'à la malveillance…

LA SÉCURITÉ MISE EN CASES

La check-list de l'OSAC répertorie 12 domaines de la sûreté/sécurité d'un établissement hôtelier, allant de sa sécurité incendie à son système de gestion de crise ou sa sécurité sanitaire, passant au peigne fin ses ascenseurs ou son centre fitness. Pour chaque domaine exploré, une série de cases à cocher est proposée. Plus on coche, meilleure est la sûreté/sécurité. En exemple, un extrait du chapitre 4 consacré au « guarding » :

- L'hôtel effectue des patrouilles périodiques de sécurité 24h/24.
- Les entrées et sorties publiques sont surveillées par le personnel de l'hôtel 24h/24.
- Le personnel de l'hôtel contrôle l'accès aux étages depuis les espaces communs.
- L'hôtel dispose d'un processus d'augmentation du personnel de sécurité sur demande en cas de réunions ou d'événements.
- L'hôtel dispose d'une garde armée sur place.
- Le personnel de sécurité de l'hôtel porte un badge.
- En cas d'urgence, le service de sécurité de l'hôtel dispose d'un gilet, d'un brassard ou de tout autre signe facilement identifiable.

L'intégralité de cette check-list peut être consultée à cette adresse : www.osac.gov.

> Si l'espionnage est une affaire aussi vieille que le voyage d'affaires ; ce qui est nouveau, c'est la cybercriminalité.

rité présente mais plus discrète, dans un quartier moins en vue ». Pas une science exacte, donc, mais de l'arbitrage fin entre avantages et inconvénients de chaque option. Mais l'arbitrage n'est jamais bien loin de l'arbitraire. Charline Gelin confirme : « *J'ai animé un workshop à plusieurs reprises s'adressant à des responsables sécurité de grands groupes. Pour le déplacement fictif d'un de leurs collaborateurs, je leur donne une liste de 3 hôtels avec leurs caractéristiques essentielles. Résultat : selon les groupes de travail, l'hôtel choisi n'est jamais le même…* »

Protéger l'information

Mais pour les clients des hôtels d'affaires, le risque ne saurait se réduire à celui d'une attaque terroriste. Le vol à la tire reste - heureusement, serait-on tenté de dire - bien plus probable, de même que celui de l'espionnage. Se prémunir du risque, c'est aussi faire preuve de discrétion dans ses échanges professionnels, et notamment éviter de parler dans des lieux publics tels que le restaurant ou le lobby de l'hôtel, même s'ils sont déserts. « *Les micros ? Il faut partir du principe qu'il y en a partout* », explique Charline Gelin qui a collaboré avec de gros groupes pétroliers présents en Afrique. Pour y remédier, des zones sécurisées et confinées existent.
Mais l'espionnage est une affaire aussi vieille que le voyage d'affaires. Ce qui est plus nouveau, en revanche, c'est la cybercriminalité. Elle devrait coûter aux entreprises 2,1 milliards de dollars en 2019 et 6 milliards de dollars en 2021, selon une étude publiée par Cyber Security Ventures. Les coffres-forts des chambres d'hôtels s'élargissent pour pouvoir accueillir l'ordinateur, à côté des traditionnels passeport et montre de valeur. Mais ce n'est évidemment pas suffisant : les agresseurs potentiels sont en mesure de contrôler l'infrastructure sur laquelle les communications circulent. Le voyageur doit donc s'assurer de la parfaite sécurisation du wi-fi qu'il utilise. C'est un critère du choix de l'établissement.
Mais pour ce type de sécurité comme pour les autres, c'est le comportement approprié du voyageur qui fait la différence. « *Le risque, c'est la route, les moustiques et nous-mêmes* », pour reprendre la formule qu'utilise plaisamment Bernard Jacquemart quand il s'agit de classer dans l'ordre les périls encourus par le voyageur. ■

CONSEILS OFFICIELS : DES TROUS DANS LE TUYAU

La cellule de crise mise en place par le ministère des Affaires étrangères en 2007 est-elle une bonne source pour préparer un voyage d'affaires ? Pas forcément…

©DR

Pourquoi ne pas s'en tenir aux recommandations du ministère des Affaires étrangères plutôt qu'avoir un onéreux recours aux sociétés de gestion des risques ?
C'est une question que peuvent légitimement se poser les travel managers avant d'envoyer leurs voyageurs à l'étranger, d'autant plus qu'un centre de crise et de soutien a été mis en place en 2007 par le Quai d'Orsay.
Mais ces conseils sont-ils les bons ? Pas toujours si l'on en croit les représentants des opérateurs en sécurité privés. L'un d'eux reproche ainsi au Quai d'Orsay d'« *assombrir le tableau pour se couvrir et éviter qu'en cas de pépin, on lui reproche un défaut de communication* ».
Le MAE pécherait donc par excès de prudence ? Charline Gelin tempère : « *Ils n'ont tout simplement pas les mêmes objectifs que nous : leur but est de protéger les Français. Nous, nous sommes des facilitateurs de business. Si un de nos clients a besoin d'aller dans un endroit à risque, nous allons l'informer, le former, éventuellement lui conseiller de reporter son voyage si la menace est temporaire, etc. Mais si ce voyage est nécessaire pour lui, notre rôle n'est pas de l'en dissuader, mais de faire en sorte d'en diminuer les risques* ».

Un centimètre qui change tout

Mais derrière l'excès de prudence peut également se cacher le défaut d'exactitude. « *Nous sommes d'accord avec 85 % des communications et des analyses du Quai d'Orsay,* précise Ludovic Guérineau. *Mais parfois on sent bien que les cartes de risques sont faites par de jeunes gens qui sortent de brillantes études mais qui ne connaissent pas bien le terrain.* » Et le professionnel de la sécurité de se remémorer une récente carte de la Mauritanie : du rouge - signifiant un risque d'attentats très élevé - recouvrait une partie du pays sans que cela corresponde, selon lui, à la réalité. « *Sur la carte, la partie rouge en trop représentait peut-être 1 cm, soit, à l'échelle, près de 150 km ! Cette région, je la connais bien, c'est un goulot d'étranglement rempli de soldats de l'armée mauritanienne : aucun risque d'attentat.* »
Petite erreur, gros effets ; cette zone indûment rougie comprenait des hôtels et vivait du tourisme. Elle est aujourd'hui désertée.

La diplomatie des couleurs

Car une communication du Quai d'Orsay peut avoir des impacts énormes. 17 000 touristes français en moins : c'est l'impact directement mesuré par le Sri Lanka d'une analyse siglée MAE en 2007. À l'époque, le système cartographique du centre de crise naissant n'avait en gros que 3 couleurs : rouge, orange et vert. Le nord et l'est du pays avaient été rougis fort logiquement vue la guerre qui y opposait le pouvoir sri lankais aux Tigres du Tamoul. Mais le reste du pays avait été rempli d'orange. Un choc pour l'office du tourisme du pays qui contacte alors Ludovic Guérineau pour obtenir un audit indépendant des risques encourus au Sri Lanka. « *J'ai parcouru le pays pendant un mois, comme un touriste, dans tout type d'hébergement. À l'issue du périple, il m'est apparu très clairement qu'en dehors de la zone de conflit, ce pays présentait des garanties comparables à celles du Maroc, par exemple* ».
Alors : fallait-il verdir l'orange sri lankais ou rendre orange le vert marocain ? Une question délicate pour un centre de crise et de soutien dont le travail de vérité reste forcément soumis à une tutelle très peu désireuse de froisser certains pays trop bons amis, trop bons alliés ou trop bons clients.