La sécurisation des infrastructures terrestres de l'énergie

Les organisations terroristes ont parfaitement compris le rôle stratégique primordial que jouent pour les nations occidentales les infrastructures de l'énergie en systématisant leurs attaques contre les sites de production et les voies de distribution du pétrole. Les sources et sites de stockage de pétrole, les robinets, les pipe-lines, les tankers et les terminaux portuaires – c'est-à-dire tous les éléments constitutifs de la chaîne logistique d'approvisionnement énergétique – forment un nœud de cibles privilégiées pour ces organisations. Nul doute que l'amplification d'un terrorisme focalisé sur des cibles énergétiques pourrait provoquer un véritable chaos économique. La gestion matérielle des flux pétroliers exige donc que soit prise en compte cette nouvelle donne et implique une sécurisation physique accrue de ces infrastructures, terrestres et maritimes, désormais soumises à la permanence de la menace terroriste. Un examen des menaces et modes opératoires susceptibles de peser sur les infrastructures de l'énergie nous permettra d'envisager les mesures à entreprendre pour prévenir les risques inhérents à la sécurité d'approvisionnement énergétique.

Typologie des menaces :

En ce qui concerne les infrastructures pétrolières statiques (puits) et de transit (oléoducs) on peut identifier deux principales menaces : le sabotage des oléoducs et l'incendie de puits de pétrole.

Le sabotage des oléoducs est la menace la plus commune et la plus importante qui pèse sur l'approvisionnement énergétique. En Afrique de l'Ouest, en particulier au Nigeria, mais également en Amérique du Sud, en Colombie par exemple, le détournement de pipe-lines fait l'objet d'une véritable économie criminelle, qui ne se restreint pas au phénomène terroriste. Les sabotages tiennent aux complicités entre les employés des compagnies exploitantes, les mafias locales chargées de la revente du pétrole au marché noir et les militaires autochtones qui fournissent la logistique pour exporter le brut ou l'essence raffinée. Les techniciens du pétrole aident les pirates en révélant les points névralgiques et le tracé des pipe-lines. Le *bunkering* – qui affecterait 5% de la production pétrolière nigériane – est la méthode la plus répandue : elle consiste à siphonner les tuyaux sans les dépressuriser, ce qui permet de ne pas alerter les exploitants.

L'incendie de puits de pétrole est un cas spécifique à l'Irak et à une situation de guerre ouverte. Lors de la première guerre du Golfe, en 1991, cette menace éco-terroriste s'était vue concrétisée par l'incendie de 700 puits,. Dans le cadre du conflit actuel, les sabotages en série des installations pétrolières font partie intégrante de la stratégie de la guérilla irakienne. L'appel de Ben Laden en décembre 2004 à intensifier les opérations de sabotage des puits et des infrastructures pétrolières en Irak et en Arabie Saoudite en est l'exemple le plus probant : « Concentrez vos opérations sur le pétrole, en particulier en Irak et dans le Golfe » disait-il. Si dans la phase d'invasion de l'opération *Iraqi freedom* cette menace semble avoir été contenue par les forces spéciales américaines (moins d'une dizaine de puits ont été incendiés), la situation d'après-guerre signale une montée en puissance des actions terroristes qui visent à paralyser la production de pétrole et empêcher une reprise des investissements. On pouvait ainsi lire dans un manifeste du parti Baas clandestin que « la bataille pour empêcher la prise de contrôle du pétrole irakien est partie intégrante de la bataille de libération de l'Irak » – http://comitesirak.free.fr/cp/cp040517en.htm.

Mesures prophylactiques :

Face à la multiplication des menaces, terroristes ou criminelles, les opérateurs ont opté pour une stratégie articulée autour des volets sécuritaires suivants : délocalisation des activités vers l'*off-shore*, renforcement technique des infrastructures, enfin recours à la coercition privée.

La délocalisation maritime de la production : l'implantation terrestre de sites d'exploitation est en effet synonyme d'une vulnérabilité accrue des infrastructures. A coup de sabotages de pipe-lines,

d'attaques à main armée, d'enlèvements de *lock-out*, voire de grèves, Shell a perdu jusqu'à un quart de sa production au Nigeria en 1999. Un tel contexte a conduit les compagnies pétrolières à opérer un repli dans des « bases-vie » et les a contraintes à un repositionnement tactique des unités de production en off-shore. Cette révision tient à un constat simple : sur le continent africain, les compagnies qui ont été les moins touchées sont celles dont la production se situait à bonne distance des côtes. Résultat, la tendance massive est aujourd'hui à des implantations *off-shore*, l'implantation *on-shore* étant rendue difficile, notamment en Afrique, par le développement d'une criminalité spécialisée dans le sabotage ou le détournement de pipelines.

Le renforcement technique des infrastructures de transport : dans le cas des infrastructures de transit terrestres, notamment les pipe-lines, l'innovation technique peut venir compenser le déficit de sécurité des installations. On peut penser à l'invention du TBK (*Tunnel Bomb Killer*) créé par la firme française SEMA. Conçu pour être enterré, ce pipe-line en tôle ondulée est composé de huit couches d'acier galvanisé réunies entre elles pour former une sorte de nid d'abeilles de 14 cm d'épaisseur, ce qui lui confère une quasi invulnérabilité aux explosifs. Naturellement ce genre de protection n'intéresse que les points d'accès jugés sensibles et ne peut couvrir toute la longueur d'un tuyau, le coût de la sécurisation s'élevant à 500 euros par mètre. Ce coût reste néanmoins très relatif si on le compare aux répercussions financières et commerciales d'un attentat sur un oléoduc – le rapport entre le coût de la protection et celui de la réparation étant de 1/100 000ème.

Le recours aux sociétés de sécurité privée : Pour les implantations non délocalisables *off-shore*, le recours aux sociétés de sécurité privée constitue la solution la plus viable et la plus évidente pour les compagnies pétrolières. Ce dernier aspect, le plus visible dans la problématique des complexes « pétro-sécuritaires », s'articule autour d'un triptyque composé à la fois de gardes privés, de forces gouvernementales autochtones et de services de surveillance internes aux entreprises. Halliburton, à travers ses filiales ESG (Energy Services Group) et KBT (Kellog Brown and Root) se sont spécialisées dans ce secteur particulièrement lucratif qu'est la sécurisation des installations pétrolières et plus particulièrement l'extinction des puits pétroliers incendiés (moins de cinq sociétés à travers le monde sont capables de mener ce type d'opération qui requiert un savoir technologique hyper spécialisé). En Irak par exemple, la société Erinys a signé avec le gouvernement américain un contrat de 39,2 millions de dollars portant sur la création d'une force paramilitaire destinée à assurer la sécurité des champs de pétrole. Erinys a ensuite fait parler d'elle en recrutant d'anciens soldats et policiers sud-africains qui avaient servi le régime de l'apartheid. Mais le contrat semble exécuté efficacement : les attaques contre les pipelines ont sensiblement baissé. L'interpénétration, dans la même chaîne de commandement, entre sociétés de sécurité privée, compagnies pétrolières et forces gouvernementales est d'ailleurs une des évolutions majeures de ce que les Américains théorisent sous l'appellation de « guerres de quatrième génération », dont l'Irak constitue la matrice.

La sécurisation des infrastructures maritimes de l'énergie

« *Si un bateau qui ne nous a pas coûté 1000 dollars est parvenu à dévaster un pétrolier de cette taille, imaginez l'ampleur du danger qui menace l'artère commerciale de l'Occident que constitue le pétrole […] Cette opération n'est pas seulement une attaque contre un pétrolier, mais également une attaque contre les lignes de transport internationales de pétrole et toutes ses différentes connotations* ». Voilà ce qu'on pouvait lire dans un communiqué du bureau politique d'Al-Qaïda qui commentait l'attentat commis en 2003 contre le superpétrolier français Limburg, au large du Yémen, preuve s'il en est que le terrorisme maritime n'est plus une hypothèse de méthode mais bien un axe stratégique de l'hyper terrorisme. D'après les services de renseignement américains Al-Qaïda disposerait en propre d'une flotte de quinze navires de haute mer. Cette évolution amène à s'interroger sur la conjonction de la piraterie et du terrorisme et les conséquences qui peuvent en découler pour la sécurité d'approvisionnement énergétique.

➢ **<u>Typologie des menaces</u>** :

⇨ ***Les attaques-suicides par de petites embarcations***, de type Zodiac, ***contre des navires pétroliers***, comme dans le cas du Limburg ou de l'USS Cole, offrent aux organisations terroristes un biais efficace pour fragiliser et mettre en échec le système de transport énergétique. Comme le souligne le communiqué très pragmatique d'Al-Qaïda le rapport de l'impact en termes de coût est un argument supplémentaire qui plaide en faveur de cette hypothèse. L'intervention de plongeurs pour déposer des bombes sous la coque d'un pétrolier est également une solution envisageable pour les terroristes (d'après Aegis, une société de conseil en sécurité britannique, le groupe islamiste philippin Abu Sayyaf aurait formé plus de quarante nageurs de combat).

⇨ On peut aussi craindre ***le détournement d'un tanker transformé en bombe flottante*** aux mains de terroristes. Butaniers et propaniers se prêtent spécifiquement à ce genre d'attentats. Les dégâts, contre des infrastructures portuaires, industrielles, voire même des plates-formes pétrolières, pourraient s'avérer absolument considérables. Une hypothèse corrélée serait l'échouage volontaire d'un pétrolier au cœur d'un détroit ou à l'entrée d'un port, qui allierait dégâts économiques et écologiques.

⇨ Sachant que 2% seulement des conteneurs qui pénètrent sur le territoire américain sont contrôlés, ***la possibilité la plus dangereuse reste que les terroristes dissimulent une bombe radiologique ou une arme de destruction massive***, munie d'un système de positionnement par satellite, ***dans l'un des 230 millions de conteneurs qui transitent chaque année dans les ports du monde***. Une fois introduite dans le réseau de transport international, via des pavillons de complaisance par exemple, il serait aisé de l'actionner à distance au moment de son arrivée au cœur d'une zone habitée. Il suffirait pour conduire une telle opération de quelques agents infiltrés parmi les dockers, voire parmi les marins (80% des certificats décernés sont des faux), placés à des points stratégiques, et dotés d'une compréhension minimale du fonctionnement de la sécurité portuaire.

➢ **<u>Mesures prophylactiques</u>** :

Suite au 11 septembre et à l'attentat contre le Limburg, la mise en œuvre de mesures de sécurité renforcées a été quasi immédiate. ***La principale difficulté de cette sécurisation consistait à pouvoir délocaliser les contrôles, c'est-à-dire à s'assurer, non pas à l'arrivée dans les ports occidentaux, mais bien plus en amont, au port d'embarquement même, que les marchandises ne présentent aucun risque***. Ce processus de sécurisation de la chaîne d'approvisionnement, initié par les Etats-Unis, s'est traduit par l'augmentation de l'annexe « Sûreté » de la Convention Solas pour le transport maritime, l'adoption de mesures unilatérales (*Container Security Initiative* ou CSI, *Custom Trade Partnership Against Terrorism* ou C-PAT) et multilatérales tel le code ISPS (*International Ship*

and Port Facility Security) qui renforcent considérablement les mesures existantes, tant à bord des navires que dans les ports,

⇨ *la sécurisation des marchandises* : ***Le CSI vise à permettre un contrôle de l'origine et des caractéristiques des marchandises ainsi que de l'identité des chargeurs et des réceptionnaires***. Ces mesures impliquent que le conteneur doit arriver au moins 24 heures à l'avance, que l'embarquement en dernière heure n'est plus possible, enfin que les armateurs doivent déclarer leur manifeste de sortie 24 heures avant l'appareillage***. Des mesures de scanning et de détection (Sycoscan) ont également été mises en place*** pour faire face aux risques d'un conteneur piégé. Reste que ces mesures sont très relatives puisqu'elles ne concernent que les conteneurs exceptionnellement suspects ou signalés comme dangereux et ne suffisent pas infirmer la tangibilité de cette menace (sécuriser toute la chaîne du fret maritime et scanner tous les conteneurs mettrait fin à la fluidité sur laquelle repose l'activité économique des ports).

⇨ *le contrôle des personnels maritimes* : En ce qui concerne les zones d'accès restreint, la mise en place de mesures d'identification biométrique a été accélérée. ***Pour ce qui est de la sûreté des équipages, il a été décidé la mise sur pied d'un système sécurisé d'identification***. Cette nouvelle pièce d'identité des marins est censée remplacer l'actuel livret professionnel maritime et permettra de vérifier l'identité et la qualité des marins, tout en facilitant leur déplacement en dehors du territoire national.

⇨ *la « stérilisation » des vecteurs de transport* : Pour les navires de transport, on peut citer l'adoption des mesures suivantes qui forment un dispositif de « stérilisation » efficace : ***la création d'un système d'identification automatique*** (*l'Automatic Identification System* qui oblige les navires à s'équiper de transpondeurs) et d'un système d'alerte, l'identification du navire par marquage sur la coque, l'établissement d'une fiche synoptique continue, ***la désignation et la formation d'un agent de sûreté à bord,*** l'établissement d'un plan de sûreté du navire, l'instauration d'une déclaration de sûreté, l'obtention d'un certificat de sûreté, et l'introduction de niveaux de sûreté dans les opérations maritimes.

⇨ *l'adéquation des infrastructures portuaires à la sûreté* : Pour les infrastructures portuaires, ***les gouvernements*** réunis au sein de l'Organisation Maritime Internationale ***se sont engagés à ce que chaque terminal portuaire fasse l'objet : d'une évaluation des risques ; de l'élaboration d'un plan de sûreté*** (gradué selon trois niveaux de menace) ; ***de la désignation d'un responsable sûreté*** (qui sera le correspondant de l'officier de sûreté que le code ISPS impose à bord de chaque navire) ; d'une formation appropriée et d'exercices périodiques.