CYBERTERRORISME :
POSSIBLE ET ...

par Daniel Martin Président fondateur de l'Institut International des Hautes Etudes de la Cyber criminalité

LE CYBER TERRORISME EST POSSIBLE ET VRAISEMBLABLE

Daniel Martin, Conseiller spécial du Directeur exécutif de l'OCDE, Président fondateur de l'Institut International des Hautes Etudes de la Cyber criminalité (Cyber crime Institute), développe la notion de nouvelle menace qui ajoute à une liste déjà longue de menaces nucléaires, biologiques, chimiques, celles qui sont liées à la dépendance accrue de nos systèmes de protection à l'égard de l'informatique.

La tragédie du 11 septembre marque la fin d'une période commencée en 1989 avec la chute du mur de Berlin et l'effondrement de l'Empire Soviétique. Nous savions déjà que nos ennemis traditionnels étaient devenus des partenaires et que nos alliés s'étaient transformés en concurrents féroces. Nous sommes rentrés brutalement dans l'ère de la guerre terroriste et criminelle. Surprise pour le plus grand nombre, dure réalité pour ceux qui avaient analysé les signaux annonciateurs de tragédie et de terreur.
Car ne nous trompons pas, ces signaux existaient :

" La prochaine fois, ce sera très précis et le World Trade Center continuera d'être une de nos cibles aux Etats-Unis si nos demandes ne sont pas satisfaites " indiquait Nidal Ayyad, militant islamiste, lors de son procès à New York en février 1993.
La Rand Corporation, think tank de la CIA avait envisagé comme un scénario possible la chute d'un aéronef sur une tour.
Que dire de Tom Clancy qui décrit par le détail de tels événements, en particulier dans un ouvrage " Sur ordre " paru en 1997.

Les actes de terrorisme brutaux ne manquent pas dans le monde :

- Mars 93, Inde, Bombay plusieurs voitures motos et valises piégées explosent simultanément : 320 morts et plus de 1200 blessés.
- Avril 95, Oklahoma city, 168 morts.
- Roubaix, France, fin 95, le Nord connaît une vague de vols à main armée sanglants dont les auteurs sont des jeunes convertis à l'islam et qui financent la cause islamiste.
- Décembre 94, des moudjahidins du GIA détournent à Alger un Airbus d'Air France. Ils sont neutralisés à Marseille par le GIGN. Leur objectif : faire sauter l'avion au-dessus de la capitale ou le précipiter sur un monument symbolique.

On peut citer aussi des plans découverts à temps.
Comme "l'opération Bojinca."
Plan découvert à Manille en janvier 95. Objectif : faire exploser 11 avions de ligne appartenant aux compagnies américaines reliant l'Asie à la Californie. Nombre prévisible de victimes : 4000 en 48 heures.

C'est déjà grâce à la saisie d'un ordinateur portable, celui de Ramzi Youssef (rappelons qu'il s'agit du concepteur du premier attentat du World Trade Center) que ce complot est déjoué.
En décembre 94, le principe est testé en grandeur réelle. Le 11, une bombe explose dans un avion de Philippines Airlines reliant Manille à Tokyo. C'est Ramzi lui-même qui place la bombe avant de descendre à Cebu où l'avion fait escale. L'avion repart et la bombe explose. Mais le pilote parvient à poser l'appareil en

catastrophe à Okinawa. Bilan 1 mort et 10 blessés.
Sur l'ordinateur de Ramzi, d'autres projets tout aussi terroristes : 2 de type Bojinka : attentats à la bombe simultanés contre 2 Boing 747 au-dessus de l'aéroport Kaï Tak de Hong Kong. et déjà, un jeune pakistanais ayant un brevet de pilotage devait s'écraser avec un avion de tourisme sur le quartier général de la CIA à Langley près de Washington.
Les informations contenues dans les ordinateurs existaient, annonciatrices du 11 septembre.

A) Les NTIC, une formidable opportunité

La mondialisation a déjà un terrain de prédilection : celui du monde virtuel. Disparition des dimensions du temps et de l'espace : tout se fait à la vitesse électronique sans tenir compte des frontières et des barrières juridiques ou culturelles ! Si on ajoute la possibilité d'avancer masqué, c'est à dire d'une manière quasi anonyme ou difficilement identifiable, alors on a un formidable outil pour les criminels.

Des conditions favorables à l'utilisation de l'outil par le terrorisme

Au plan technique

La communication est un facteur primordial pour les réseaux, qu'il s'agisse d'espionnage, de criminalité organisée de type mafieux ou encore de terrorisme. Internet, les matériels informatiques de plus en plus puissants associés à des logiciels performants constituent des outils rêvés pour communiquer rapidement partout dans le monde tout en restant discret. ETA, le mouvement terroriste basque, l'a bien compris, utilisant pour ses transmissions des algorithmes de chiffrement incassables par les services gouvernementaux. Les mafias utilisent depuis longtemps les ressources de la stéganographie qui permet de cacher des messages dans des textes, images ou morceaux musicaux. Enfin, tout ce qui est binaire. On sait que les réseaux Ben Laden ont eu recours à de tels procédés, tout en poursuivant en parallèle l'utilisation de méthodes archaïques comme l'envoi de faucons à travers les frontières séparant le Pakistan de l'Afghanistan.

A Londres, en mai 97, une opération conjointe du MI 5 et de l'unité antiterroriste de Scotland Yard a permis de saisir du matériel informatique sophistiqué qui démontrait déjà l'utilisation de ces moyens pour à la fois synchroniser les opérations et garantir un prosélytisme ardent des idées terroristes.
On ne peut pas non plus éviter de souligner qu'Internet est le support de sites particulièrement dangereux où l'on trouve aussi bien la méthode de fabrication d'une bombe artisanale que celle d'une bombe électromagnétique avec la liste des produits qui la composent, en vente libre dans le commerce. Ce type de bombe est capable, pour quelques centaines de dollars, d'effacer toutes les données stockées sur des supports magnétiques. On imagine les dégâts !
Compte tenu de ce qui existe sur le marché, pratiquement n'importe qui peut se procurer, en vente libre, pour un investissement ridicule par rapport au coût des armements classiques, les moyens d'attaquer ou de détruire les systèmes d'information d'un pays et de mettre à genoux une grande puissance ou une multinationale. L'équipement de base du terroriste est simple : un micro ordinateur, une connexion au réseau. Le savoir-faire offensif peut être puisé sur internet ?

Au plan humain

Les pays ou organisations en cause en matière terroriste disposent d'une intelligentsia d'excellent niveau. Arrêtons de croire que les volontaires au sacrifice ultime sont des simplets au cerveau lavé. Les 19 bombes humaines du 11 septembre sont toutes issues de milieux bourgeois. Ils ont fait des études en

occident, parlent plusieurs langues, ont un métier, sont apparemment bien intégrés dans la vie active. Ils ne se font pas remarquer. L'hebdomadaire égyptien Al Watan Al Arabi le rappelait déjà en octobre 95 : les islamistes ne sont pas tous des analphabètes. Une majorité d'entre eux, responsables et militants confondus ont même suivi un cursus scientifique. A titre d'exemple, on sait que Ramzi Youssef est ingénieur en électronique, que son complice Hakim Mourad est diplômé de l'Académie aéronautique de Caroline du nord. Rabah Kebir, chef de la délégation parlementaire du Front Islamique du Salut (FIS) était lui-même diplômé en physique.
Si on ajoute le fait que de très nombreux étudiants étrangers en provenance des pays à risque ont été formés dans nos pays (en dix ans, plus de 4000 informaticiens de niveau DEA ou DESS) et qu'ils ont pour la plupart effectué des stages en entreprise, parfois dans des secteurs sensibles, alors on est obligé d'admettre qu'ils connaissent ainsi les outils et les matériels employés, les habitudes des personnels, la culture d'entreprise et donc les failles susceptibles d'être exploitées .

Au plan international absence de réelle coopération efficace

Depuis la chute du mur, les services, très orientés " Est " ont du mal à faire leur mutation. Bien sûr, les échanges existent, souvent bilatéraux ou au sein de Clubs, mais chacun joue sa partition et ne dévoile pas ses atouts. On est dans un climat de guerre économique où tous les coups sont permis pour gagner des marchés. Disons le tout net, la coopération n'est pas très efficace, même si elle existe. Alors dans ce contexte, le terrorisme bénéficie d'une garde assez basse.

Une situation léthargique des USA

Les Etats-Unis étaient jusqu'à la tragédie du 11 septembre pratiquement un sanctuaire. Les difficultés, les actes de guerre, c'est pour les autres, sur d'autres territoires, d'autres continents, d'autres pays.
On a tout misé sur le High Tec et l'électronique. ECHELON veille avec ses satellites espions qui écoutent toutes les transactions, du téléphone portable à l'e-mail. Les ordinateurs de la NSA dévorent l'équivalent de la bibliothèque du Congrès, la plus grande du monde toutes les trois heures. Des interprètes traduisent les échanges dans plus de 90 langues. Mais encore faut-il exploiter d'une manière cohérente toutes ces données et prendre, dans les délais impartis, les décisions utiles. AOL transporte chaque jour 225 millions de courriers électroniques et 1,1 milliards de messages instantanés. Pour les seuls USA, les communications téléphoniques cellulaires en 2000 représentaient 2,58 milliards de minutes ! On comprend les limites du système.

En réalité, çà ronronne. La CIA est en plein engourdissement intellectuel. La théorie du " politically correct " a tué les vieilles méthodes. Le recrutement d'un agent est un véritable casse-tête bureaucratique. Celui issu d'un milieu criminel ou terroriste (human rights violator) découragé, voire interdit. Les instructions (assets validation system) sont consignées dans un manuel de plus de 40 pages ! On peut même dire qu'aucun projet sérieux d'infiltration de clandestins dans une organisation fondamentaliste islamique n'a été mis en œuvre avant le drame. Alors ne parlons même pas des illégaux, les " non official cover " qui, installés à leurs risques et périls dans le privé ne bénéficient d'aucune couverture. Risques majeurs, ils ont quasiment disparu ! Encore une fois, on mise sur le technique en créant plutôt un centre " global response Center " pour tuer dans l'œuf les initiatives terroristes en brisant les réseaux, compliquant les déplacements, neutralisant les transferts d'argent, l'achat de matériels. Les services se sont éloignés de la réalité. On nage dans le Wargame. Le renseignement humain est négligé alors que la technologie est incapable de mesurer le degré de haine, d'envie, de jalousie et que toute manipulation est

fondée sur des règles humaines : le A I S E (argent, idéologie, sexe et ego..) ou la règle des 3 c (cerveau, cœur, etc.). Les Etats-Unis ont perdu le sens du concret et résident dans une sorte de monde virtuel.

Pourtant, une Europe expérimentée et en alerte avec ses moyens limités
Les vieux pays européens font face depuis longtemps à des actes de terrorisme. Rappelons nous la bande à Baader en Allemagne, les brigades rouges en Italie, ETA et les autonomistes basques en Espagne, les vagues d'attentats islamistes en France. L'IRA en Angleterre, pour ne citer que les plus importants.
Les services ont appris à faire face devant les faits. Et ils ont beaucoup appris. Le manque de moyens aiguise l'intelligence. La faiblesse des moyens techniques a été épaulée par les bonnes vieilles techniques de l'entrisme, de l'infiltration et de la manipulation humaine. Les résultats sont là.
C'est ainsi que plusieurs des services spécialisés européens, SISMI et SISDE italiens, DST et DGSE français, CESID espagnol, BND ET BFV allemands ou encore MI5 et MI6 britanniques ont fait parvenir des informations concordantes sur les possibilités d'actes de terrorisme sur le sol des USA. Il semble que ces avertissements n'aient pas été pris au sérieux ou encore que les circuits de décision et d'information complexes n'aient pas permis une prise en charge de ces éléments.

Des opportunités certaines favorisent l'émergence d'un cyberterrorisme: les vulnérabilités de nos infrastructures sensibles

Des exercices de cyber attaques sont depuis plusieurs années développés par plusieurs pays. La menace n'est pas seulement virtuelle, plusieurs secteurs sensibles de nos sociétés hyper automatisées ont été mis en exergue : l'énergie (production, transport et stockage des hydrocarbures et de l'électricité, transports, télécommunications, systèmes financiers, approvisionnement en eau, services gouvernementaux fondamentaux et services d'urgence (pompiers, police, médecins).
On imagine les conséquences : plus d'électricité, plus rien ne fonctionne. On sait la place tenue par les transports dans nos sociétés fondées sur les échanges ! Trafics aériens, ferroviaires ou routiers perturbés. Que dire des services financiers : il suffit de se rappeler notre degré d'autonomie financière : combien de liquide dans nos poches ? Alors si les cartes bancaires ne marchent plus, comment faire ? Et si brutalement les virements sociaux n'arrivaient plus ? Plus d'allocations familiales, plus de prestations ! Combien de temps un gouvernement pourrait-il tenir ? Les grandes banques ne maîtrisent plus toutes les chaînes d'information et de communication. 72 des 100 plus grandes banques américaines externalisent une partie de leurs fonctions essentielles. La moindre défaillance d'un des sous-traitants peut mettre en danger toutes les banques qui recourent à lui.

Ainsi, on voit se profiler les termes d'une sorte de terreur informatique. Plus rien ne marche, tout est bousculé. Et si cette attaque se produit en complément d'un acte de terreur classique, un attentat par exemple, alors on imagine que les effets sont décuplés. Il suffit de se rappeler AZF et Toulouse. Peu importe les causes, accident, malveillance ou acte délibéré. Imaginons alors une désorganisation des services de secours. Ce fût d'ailleurs une leçon, car le téléphone, à part celui dépendant des moyens gouvernementaux ne fonctionnait plus.

b>Des outils favorisant les échanges
Les circuits financiers sont des utilisateurs privilégiés des réseaux électroniques. Aujourd'hui, il faut moins de 10 minutes à un gros virement pour faire le tour de la terre en passant pourtant par de multiples banques. On ne peut pas ici omettre de parler du financement du terrorisme qui a recours à tous les outils proposés sur le marché.
Il faut alimenter les réseaux de soutien, entretenir les caches, payer les agents,

acheter certaines complicités. Il faut beaucoup d'argent. On a pu remonter certains circuits. Le terrorisme utilise les mêmes méthodes que les blanchisseurs d'argent, mais souvent aussi à l'envers. On peut ici parler de noircissement d'argent propre. L'argent récupéré à la sortie de lieux de culte, celui issu de certains comptes de sympathisants (réels ou forcés !) est ensuite sorti des circuits normaux pour alimenter des filières d'achat d'armes ou pour commettre des actions illicites.

On a pu aussi déterminer que Mohamed ATTA, l'organisateur des attentats du 11 septembre a utilisé la Western Union, une banque qui se vante d'être la plus rapide et la plus sûre pour faire transiter de l'argent d'un point à l'autre du globe à travers ses 118000 agences, sans contrôle en dessous d'un seuil élevé (15000 Euros). Au moins à deux reprises, Mohamed ATTA a fait parvenir de l'argent à des correspondants aux Emirats Arabes Unis. Et ici on mesure la difficulté de contrôler avec efficacité le financement des réseaux. Rien ne distingue ces mouvements d'autres mouvements normaux. Et il faut tout éplucher. Et aussi souligner que ces systèmes sont largement utilisés par les mafias et pour les opérations de corruption qui minent nos sociétés.

Vers un passage à l'acte prévisible

Tous les ingrédients sont réunis, les scénarios développés.
En voici un, déjà ancien, mais toujours d'actualité :
" L'Iran choisi de porter l'attaque sur le sol des USA et décide de s'attaquer à son point faible : les systèmes d'information. Rapidement, les centraux téléphoniques de certaines bases militaires deviennent inutilisables, saturés par des virus et mis hors service par des bombes logiques placées à distance depuis déjà un certain temps par des pirates agissant depuis plusieurs pays distincts et alliés des USA. Des trains déraillent suite à des défaillances du système de contrôle du trafic ferroviaire. Les avions sont collés au sol. Les logiciels de traitement des billets sont inopérants, on ne sait plus enregistrer les bagages. Plusieurs centres météo tombent en panne. La banque centrale découvre une tentative de sabotage de son système de transfert de fonds. Lorsque CNN annonce que les Iraniens ont payé des informaticiens russes et des programmeurs indiens pour détruire l'économie occidentale, les cours des bourses de New York et de Londres s'effondrent. Plusieurs grandes banques sont piratées. Mouvement de panique chez les épargnants qui veulent retirer leurs dépôts. Des programmes pirates de propagande inondent les chaînes de télé privées. Washington est privé de téléphone, le Président lui-même a du mal à réunir ses conseillers?

Ce n'est qu'une fiction où sont placés bout à bout à peu près ce que l'on saurait faire aujourd'hui pour neutraliser un pays.

Des signes avants coureurs existent. Vous avez sans doute lu dans la presse récemment, cette mise en garde de la part d'un fabricant de logiciels anti virus, attirant l'attention des pouvoirs publics sur une génération de virus ou plutôt de chevaux de Troie destructeurs et indétectables par les moyens actuels. Ce n'est pas qu'une opération commerciale. Un jour ou l'autre, on va voir surgir des tueurs de disques durs, des éliminateurs de fichiers.
Mais alors à quel ennemi a-t-on à faire ?
Un nouvel ennemi, mais lequel ?
Le terrorisme est multiforme et on ne peut négliger aucune hypothèse. Le terrorisme peut être individuel, de groupe ou encore étatique.

Individuel certainement, et difficile à repérer et à éradiquer. La vague de lettres à l'anthrax en est l'illustration. Rappelons également le temps mis par le FBI pour neutraliser " Unabomber ".qui en 15 ans a envoyé une vingtaine de colis piégés et provoqué la mort de trois personnes avant d'être neutralisé.
Autre exemple, les " fanatiques de la nature " constituent un des groupes à risque. Ils ont déjà tenté d'empoisonner des réservoirs d'eau et des ventilations

d'immeubles. Rappelons-nous aussi la secte Aum au Japon. Et bien sûr des mouvements comme Al Qaïda.

Mais la menace terroriste surtout en matière informatique peut provenir des états eux-mêmes !
Qui est mieux placé pour mener une attaque dans ce domaine ? Qui développe les outils, les logiciels, contrôle les réseaux ? Qui élabore les scénarii de défense ? Peut-on se défendre sans mettre en place des répliques et donc sans envisager le volet offensif ?
L'Amérique a compris depuis longtemps que les pirates sont des armes offensives efficaces et redoutables. L'ancien patron de la CIA ne disait-il pas que l'électron est la munition du XXIème siècle ? Et quand il parlait d'électron, il pensait aux électrons des ordinateurs, à l'ère de l'information.
Pour lui, les pirates sont les nouveaux guerriers de l'Amérique.
L'arme numérique est très utile dans le cadre d'une confrontation. C'est le numéro 1 des services secrets allemands qui le dit :
" Tous les pays sont en train de développer leurs propres virus pour paralyser ou espionner les systèmes des autres pays, et de former des soldats au piratage informatique ".
Aujourd'hui, une trentaine de pays sont capables de mener une véritable guerre informatique et si la menace terroriste de groupe doit être prise eu sérieux, l'attaque par un pays majeur dans ce domaine ne doit pas être négligée. Elle est vraisemblable !

Le danger réside surtout dans un conflit asymétrique.

Les USA attaqués par un mouvement ou un groupuscule situé au Soudan par exemple. On imagine les difficultés de réaction.
On n'envoie pas les chars Leclerc contre les hackers d'Internet, on n'utilise pas la bombe atomique contre les sectes, les fantassins sont inutiles sur les réseaux !
Si une véritable cyber dissuasion est envisageable entre pays hyper automatisés, il sera difficile et risqué de riposter à une attaque de ce type.
C'est la raison pour laquelle nous avons intérêt à une automatisation la plus poussée possible de tous les pays afin de pouvoir faire pression sur leurs infrastructures en cas de besoin. A ce moment là, les moyens existent pour réagir efficacement.

Organisation de la riposte.
Comment faire face. Une prévention est-elle possible ?
Plusieurs actions sont à prendre, en voici quelques unes :
Réorganiser les fonctions de renseignement
Les services ont montré leurs limites. Il est nécessaire de tirer les enseignements des erreurs commises. Pour une meilleure efficacité, il faut sans doute ramasser les structures, regrouper les centres multiples d'analyse. Le FBI vient de montrer le chemin. Les 11 directions existantes viennent d'être ramenées à 4 principales : lutte contre l'espionnage et le terrorisme, ordre public, gestion des ressources et cybercriminalité.

Réorienter les outils de réaction.
Les militaires classiques ne sont pas la meilleure riposte. Le monde civil est visé et impliqué.
Il est nécessaire de se montrer très rapide dans les réactions et très souple.
La veille 24 heures sur 24 et 7 jours sur 7 est indispensable, avec des équipes bien formées en réseau et des partenaires dans tous les pays alliés.
Le G8 dans sa structure de lutte contre la cybercriminalité a initié une initiative de ce type. Elle est déjà en cours d'implantation.

Supprimer la grande différence entre sécurité intérieure et extérieure.

Aujourd'hui, la sécurité est un concept global, il faut que les structures tiennent compte de ces réalités. Aller vers la suppression des compétitions malsaines entre services

Repenser la coopération internationale
Vers une efficacité certaine. Aujourd'hui, toutes les structures s'emparent du sujet et c'est le trop plein. Uniquement sur le créneau de la corruption et du blanchiment d'argent, j'ai dénombré plus de 40 organismes divers qui œuvrent sur le sujet. Ramasser les compétences devient urgent. Le risque est international et on ne peut que souhaiter une réaction unitaire. Pourquoi ne pas franchir le pas et avoir le courage de proposer une seule structure opérationnelle capable de contenir tous les éléments utiles à la compréhension et à l'élaboration de solutions acceptables ?

Redéployer les moyens,
Les moyens à dégager sont énormes et aucun pays n'a les budgets suffisants pour faire face, seul, au problème. Il faut donc faire preuve d'imagination et envisager des solutions nouvelles, des programmes communs de développement. Sans doute aussi des outils ou des armes nouvelles. Les USA viennent de quadrupler les budgets de recherche et développement. Oui, les budgets ont été multipliés par 4 ! On imagine les conséquences dans quelques années sur les industriels de l'armement en Europe.

Rééquilibrer l'équation entre renseignement technique et renseignement humain
L'absence de ressources au niveau des agents a fait gravement défaut. Il faut revoir les méthodes et favoriser le recrutement de sources humaines, l'infiltration des mouvements. Ceci va prendre du temps, mais c'est prioritaire !

Rétablir une vraie fonction de contrôle des sources
En contrepartie, il devient alors nécessaire de vérifier et analyser scrupuleusement toutes les informations recueillies. C'est un vrai métier qu'il va falloir remettre aussi au goût du jour pour éviter l'intoxication et la désinformation en provenance de l'adversaire.

Etablir un climat de confiance entre partenaires
Même avec des divergences, les démocraties sont capables de dégager des axes forts de valeurs communes. Encore faut-il avoir confiance.

Revoir l'éthique
Une charte de bonne conduite apparaît indispensable aussi. Le sentiment de supériorité des USA est mal vécu par nombre de ses partenaires, amis et alliés. Sans respect mutuel, peu d'efficacité. Des progrès sensibles sont à faire dans ce sens, et malheureusement, aujourd'hui, la plus grande puissance du monde ne semble pas orientée dans le bon sens.

Conserver un pouvoir d'information indépendant et fiable
C'est la raison pour laquelle nous devons veiller à une indépendance certaine afin de forger nos propres appréciations. L'Europe a la chance, encore, d'avoir des vecteurs de lancement, des satellites, enfin d'avoir des yeux et des oreilles.

Contrôler avec rigueur les circuits financiers
Examiner à la loupe tous les fichiers des rares sociétés de clearing qui emmagasinent toutes les transactions financières et réalisent les compensations interbancaires. Elargir les pouvoirs du GAFI en y rajoutant une part essentielle de renseignement et en lui confiant un pouvoir coercitif. En un mot, arrêter d'utiliser les mêmes outils et les mêmes places financières que les criminels.

La partie n'est pas simple. Après le 11 septembre, on a comme une défiance envers les services de renseignement et les technologies. On parle même d'une

sorte de trahison de la technique. ECHELON, çà sert à quoi si on n'a rien vu venir ? Il ne faudrait pas pour autant que le balancier reparte de l'autre côté et que l'on sous-estime ces menaces technologiques.
Les outils d'attaque et de déstabilisation existent. Un jour ou l'autre ils seront utilisés à des fins néfastes ou criminelles. L'attaque cyberterroriste n'est pas un tigre de papier. Elle est possible et vraisemblable.
On a vu le "low tec", voire le "no tec" à l'œuvre. On a détourné des avions devenus des bombes volantes avec de simples cutters.
Ceci ne veut pas dire que la menace "high tec" n'existe pas.

J'encourage les gouvernements à réfléchir sur les dépendances vis à vis des NTIC. Les risques engendrés sont dramatiques. Je demande l'inscription d'un I supplémentaire dans la liste des menaces majeures : Nucléaires, Biologiques, chimiques et maintenant **INFORMATIQUES**. Si les gouvernements ne peuvent ou ne veulent faire face seuls à ces menaces, alors il faut faire appel à des structures privées, pourquoi pas du type ONG qui peuvent dans un esprit de transparence et de grande liberté échafauder des esquisses de solution sans être empêtrées dans des considérations politiques.
C'est une des raisons pour lesquelles j'ai fondé le CYBERCRIMINSTITUT. L'Institut International des Hautes Etudes de la Cybercriminalité.

Ne nous trompons pas. **Le problème est également politique.** C'est au politique de prendre ses responsabilités et surtout pas aux services de définir eux-mêmes leurs missions. Dans une démocratie, les services doivent être sous contrôle et ne pas s'auto diriger. Il est temps d'afficher ses convictions et de la volonté.
Ethique et détermination, voici deux mots qui devraient revenir au devant de la scène, enfin on ne peut que le souhaiter. C'est la condition pour neutraliser les ennemis de la démocratie.

Daniel Martin

*** Ndlr. Les conclusions et opinions exprimées dans cet exposé sont celles de l'auteur, à titre personnel, dans le respect de la liberté expression. Elles ne reflètent en aucune manière la position d'un service public, d'une administration gouvernementale ou d'une organisation internationale**

Daniel MARTIN est commissaire Divisionnaire Honoraire de la Police Nationale, Conseiller spécial du Directeur Exécutif de l'Organisation de Coopération et de Développement Economiques (OCDE), président fondateur de l'Institut International des Hautes Etudes de la Cybercriminalité (Cyber Crime Institute).

Courtoisie de l'Académie de la Paix et de la Sécurité Internationale

www.geopolitis.net