La guerre de l'information (I)*

L'importance de l'informatique pour le fonctionnement de nos sociétés est manifeste. Les ordinateurs se retrouvent dans – et contrôlent souvent – presque toutes les activités, allant du fonctionnement de l'Etat aux transports, de la fourniture d'énergie au secteur financier, des télécommunications à la gestion des ressources hydrauliques.

Le rythme de cette évolution est des plus impressionnants ; il aura fallu 35 ans à la radio et 13 ans à la télévision pour connaître une utilisation de masse, contre 4 années seulement à Internet.

La dépendance de nos sociétés envers les ordinateurs et le fait que de nombreuses infrastructures vitales sont ainsi interconnectées par voie électronique posent des problèmes évidents de sécurité. C'est ainsi qu'un terme nouveau a fait son apparition : *la guerre de l'information*.

Par analogie avec la « guerre biologique et le bioterrorisme » que nous vous avons présenté il y deux mois, nous verrons ici qu'il convient d'envisager l'existence d'une *guerre de l'information* et de l'*infoterrorisme*. Pour ce faire, ce document aborde les menaces y associées. Dans une seconde partie, publiée dans le prochain numéro du Ban, nous passerons en revue les initiatives prises en vue de les contrer.

Commençons d'abord par souligner la différence qui existe entre l'utilisation de l'information (désinformation) lors d'un conflit et le concept plus récent de *guerre de l'information*. La première notion, connue depuis l'antiquité, fait fondamentalement référence à l'intoxication tactique et stratégique, à la propagande de guerre et à la destruction des systèmes de commandement et de contrôle. Quant au concept plus actuel de guerre de l'information, il va bien au-delà du champ de bataille traditionnel et ses auteurs et victimes éventuels ne se limitent en aucun cas au domaine militaire.

L'*Institut pour l'étude avancée sur la guerre de l'information* propose la définition suivante : "La guerre de l'information consiste en l'utilisation offensive et défensive d'informations et de systèmes d'information afin d'exploiter, d'altérer ou de détruire les informations et les systèmes d'information de l'adversaire, tout en protégeant les siens. Des actions de ce type sont destinées à obtenir des avantages sur des adversaires militaires ou commerciaux."

De son côté, l'*International Centre for Security Analysis* du King's College de Londres distingue plusieurs niveaux qui reprennent, entre autres, les deux aspects retenus ci-avant :

- Un premier niveau qui "couvre toute la gamme de techniques psychologiques, médiatiques, diplomatiques et militaires destinées à influencer le mode de pensée d'un opposant, que celui-ci soit un chef militaire ou une population entière".

* Extrait du projet de rapport général « Information Warfare and International Security », Commission des sciences et des technologies de l'OTAN, avril 1999.

- Un autre niveau où l'accent est mis sur n'importe quel type d'attaque contre des infrastructures d'information civiles ou militaires, y compris le piratage informatique ou le craquage des codes (intrusion délictueuse), l'interruption des flux de données, l'intrusion dans des systèmes d'information, ainsi que la destruction physique, l'intoxication et les opérations psychologiques.

Rappelons aussi qu'une attaque de ce genre peut provenir de l'extérieur ou de l'intérieur de l'organisation ou du système visé. Ensuite, rappelons que l'on peut distinguer des attaques de quatre catégories :

- Les *attaques à l'aide de données*. Celles-ci ont lieu en insérant des données dans un système pour provoquer son mauvais fonctionnement.
- Les *attaques à l'aide de logiciels*, similaires aux attaques à l'aide de données, ont lieu en chargeant des logiciels dans des systèmes et entraînent leur mise hors service ou leur font effectuer des fonctions différentes de celles auxquelles ils sont destinés.
- Le *piratage ou le craquage* consiste à prendre ou à tenter de prendre le contrôle d'un système d'information (ou d'une de ses parties vitales) pour interrompre son fonctionnement, refuser son utilisation, voler des ressources ou des données, ou causer tout autre type de dommages.
- Les *attaques physiques* constituent la forme d'attaque traditionnelle (bombardement, prise d'assaut et destruction) dirigée contre des systèmes d'information. Les pulsations électromagnétiques (PEM) engendrées par des explosions nucléaires peuvent également être classées dans ce type d'attaque comme nous le verrons plus loin.

Toutes ces formes d'attaques menées dans le cadre de la guerre de l'information peuvent être classées en fonction de leurs buts ou de leurs objectifs tactiques : elles peuvent viser l'exploitation, l'intoxication, l'interruption ou la destruction des systèmes d'information.

De manière générale, une menace peut donc être définie comme la combinaison d'une *capacité* et d'une *intention hostile*. D'après de nombreux analystes, la crainte d'attaques contre les systèmes d'information se justifie par le fait que les moyens d'agression sont largement disponibles, peu onéreux et simples à utiliser, que ce soit par des Etats ou par de organisations terroristes ou même par des individus isolés. Dans un monde où même les gouvernements et les militaires ont tendance à se satisfaire de matériels informatiques et de logiciels standards disponibles dans le commerce [commercially off-the-shelf (COTS)], quiconque, ou presque, qui dispose d'un ordinateur et des compétences techniques requises peut devenir un pirate informatique ou un cyberterroriste.

Qui plus est, les progrès de la technologie informatique rendent les outils électroniques nécessaires pour mener de telles attaques chaque jour plus sophistiqués et plus faciles à acquérir, par le biais d'Internet et d'un monde informatique totalement interconnecté. La caractéristique la plus potentiellement dangereuse de la guerre de l'information réside toutefois dans le fait qu'elle peut être menée de n'importe où dans le monde et que les possibilités de découvrir l'origine de l'attaque, ou même sa présence, sont extrêmement limitées.

La criminalité informatique est le prélude à la guerre de l'information. En effet, les ennemis potentiels de l'Occident ne se limitent plus aux seuls Etats criminels capables de mettre au point des armes de destruction massive et aux groupes terroristes que ces Etats soutiennent souvent, mais incluent également des pirates informatiques, des organisations criminelles, des espions industriels et des terroristes indépendants.

Certains experts émettent toutefois des doutes quant à l'efficacité, la capacité ou la volonté de ces acteurs qui ne sont pas inféodés à des Etats à mener des attaques susceptibles de sérieusement menacer la sécurité nationale. Toutefois, lorsque l'on considère l'importance de la technologie informatique dans nos sociétés, il est clair que l'existence éventuelle d'une "cybermenace" ou le risque d'une "cyberattaque" doivent être pris au sérieux.

Par exemple, au cours des quinze dernières années, des systèmes d'information appartenant aussi bien au secteur public que privé ont fait l'objet d'attaques et celles-ci augmentent substantiellement avec le développement d'Internet. Les virus informatiques constituent une préoccupation majeure pour les experts de la sécurité de l'information. Ces virus revêtent généralement la forme de très petits programmes aux capacités souvent destructrices. Ils sont conçus pour envahir des systèmes informatiques ou des ordinateurs personnels en s'attachant à des segments de codes assurant l'exécution des programmes. Créés par des pirates, des étudiants en science informatique ou des programmeurs mécontents, ces virus destructeurs n'ont, jusqu'à présent, pas fait la preuve de leur efficacité comme armes. En raison de leurs origines non professionnelles, ils contiennent souvent des erreurs et leurs auteurs sont en outre souvent incapables d'envisager la complexité et la diversité des systèmes auxquels ils s'attaquent.

Il est naturellement toujours possible qu'une organisation militaire ou qu'un groupe terroriste puisse mettre sur pied une équipe d'experts capables de créer des virus nuisibles et les utilise pour mener des attaques dans le cadre d'une guerre de l'information. Les virus informatiques sont toutefois extrêmement imprévisibles et leur comportement est loin d'être précis, de sorte qu'en fin de compte, ils peuvent causer autant de dommages à l'attaquant qu'à ses victimes. Qui plus est, l'industrie antivirus internationale est aujourd'hui parvenue à pleine maturité et elle est en mesure de créer les antidotes nécessaires contre virtuellement tous les nouveaux virus.

D'autres attaques plus dangereuses contre des systèmes d'information sont menées par des pirates informatiques. Des sociétés du secteur privé, du secteur financier en particulier, sont régulièrement piratées par des cybercriminels : le FBI estime que ces intrusions électroniques entraînent chaque année des pertes de quelque 10 milliards de dollars aux Etats-Unis uniquement. Et il ne s'agit probablement là que de la partie visible de l'iceberg. En effet, le souci de veiller aux intérêts des actionnaires et de conserver la confiance de la clientèle peut empêcher de nombreuses entreprises de faire part de ces attaques aux autorités.

Les intrusions électroniques au sein de l'infrastructure informatique militaire suscitent également de graves préoccupations aux Etats-Unis. D'après le CSIS, les attaques exploratoires contre le Pentagone se comptent par dizaine de milliers chaque année. Le Secrétaire adjoint à la Défense, a récemment révélé qu'entre le mois de janvier et la mi-novembre 1998, la *National Security Agency* (NSA) a enregistré plus de 3 800 tentatives d'intrusion contre les systèmes et les réseaux non secrets du département de la Défense. Plus de 100 de ces pirates ont eu accès à l'organigramme de base de l'infrastructure et nombre d'entre eux sont même parvenus à détruire certains programmes. Il ne s'agit là que des chiffres reconnus par la NSA, mais "le nombre réel d'intrusions est considérablement plus élevé".

Si la plupart des attaques des dernières années ont généralement été effectuées par des individus ou de petits groupes d'intrus peu ou pas motivés politiquement, plusieurs cas récents suggèrent la possibilité de piratages ou de craquages parrainés par des Etats. On constate en outre certaines activités visant directement les Etats et motivées politiquement. En octobre 1998, la Chine a lancé un nouveau site web pour faire part de ses efforts en faveur des droits de l'homme. Quelques jours plus tard, des pirates ont remplacé la page d'accueil de ce site par un message condamnant Pékin pour ses violations des droits de l'homme.

Le système d'information de l'OTAN a également été indirectement menacé en novembre 1998, lorsque des pirates informatiques se sont introduits dans un serveur web en Albanie et ont fait passer un message annonçant leur intention de s'attaquer au système d'information de l'Alliance. L'Organisation a alors dû temporairement fermé tous les accès étrangers à son serveur web et son site web a été mis hors service pendant deux jours.

Plus récemment, lors des premiers jours des frappes de l'OTAN contre la Yougoslavie, des pirates informatiques se sont attaqués au site web de l'Alliance et ont entraîné une saturation des lignes du serveur en ayant recours à une "stratégie de bombardement". L'OTAN a également dû se défendre contre des virus macros provenant de Yougoslavie, qui tentaient d'altérer son système de courrier électronique. Celui-ci a également été saturé par l'envoi de 2 000 messages par jour par une seule et même personne.

De tels exemples ne suffisent peut-être pas à prouver l'existence d'une guerre de l'information ou d'un cyberterrorisme parrainé par des Etats, mais ils sont révélateurs de ce qui pourrait se passer en cas de couplage d'une compétence technique et d'une intention hostile. La question qui en découle est alors : un groupe de terroristes parrainés par un Etat ou des craqueurs individuels seraient-ils en mesure d'endommager l'infrastructure d'information d'un autre pays pour entraîner

des perturbations stratégiques majeures ? Le département américain de la Défense semble le penser.

De nombreux pays tentent d'acquérir les capacités nécessaires pour mener des opérations dans le cadre de la guerre de l'information et de nouveaux groupes terroristes tels que Osama bin Laden's utilisent des ordinateurs et des télécommunications par satellite. La Chine a récemment intensifié ses programmes de guerre de l'information afin de protéger ses infrastructures militaires et de mettre l'Armée de libération populaire en mesure de procéder à des attaques électroniques. D'après un spécialiste de la défense travaillant pour la Rand Corporation, Pékin "cherche à être capable à la fois de s'immiscer dans le système de commandant de Taiwan et de s'introduire dans les réseaux militaires américains qui contrôlent le déploiement dans la région asiatique".

Enfin, n'oublions cependant le danger des effets des pulsations électromagnétiques (PEM). Celles-ci, peuvent être simplement engendrées par l'activité solaire mais surtout lors d'explosions nucléaires et, dans ce dernier cas, représenter une grave menace physique pour les systèmes d'information. En effet, l'énergie dégagée par l'explosion d'un engin nucléaire produit des plasmas liés à d'intenses champs magnétiques et électriques à variations rapides qui peuvent se propager sur des distances considérables et gravement affecter tous les équipements électroniques et les transmissions électriques ou radars, jusqu'au point de détruire leurs circuits, leurs microprocesseurs et leurs autres composants. Il en résulte qu'une seule explosion nucléaire à très haute altitude au-dessus de l'Europe ou des Etats-Unis pourrait mettre hors service ou gravement perturber tous les systèmes d'information, sans pour autant occasionner des dommages corporels ou matériels. Si rares sont les pays qui disposent à l'heure actuelle des armes nucléaires et des missiles capables de les acheminer dans l'espace, le nombre croissant d'Etats "criminels" possédant des armes nucléaires et qui mettent actuellement au point ou acquièrent des missiles à longue portée peuvent représenter une menace PEM extrêmement sérieuse dans un proche avenir.

Les effets PEM résultant d'explosions nucléaires et d'armes non nucléaires, telles que les canons FRHE (fréquences radios à haute énergie) ou les bombes T/PEM (transformateur à impulsions électromagnétiques), peuvent être beaucoup plus dangereux pour les systèmes d'information civils que pour leurs homologues militaires, qui sont désormais pour la plupart renforcés PEM. Un blindage à l'aide de fer ou d'autres matériaux tels que des mailles de cuivre ou des métaux non magnétiques n'est généralement appliqué que sur les équipements militaires sensibles.

Comme nous l'avons vu dans ces quelques pages, ce nouveau problème doit faire l'objet d'une attention particulière. Dans une deuxième partie, présentée dans le prochain numéro du Ban, nous vous dévoilerons quelles sont les réponses américaines et européennes à cette menace.

Lt (R) Paul SCIMAR