La guerre de l'information (II)*

Au cours de l'été 1997, un exercice de simulation baptisé *Eligible Receiver* a eu lieu au Pentagone, sur ordre du chef d'état-major interarmes, afin de mettre à l'épreuve la capacité de l'infrastructure civile et militaire nationale à résister à une attaque concertée s'inscrivant dans une guerre de l'information. L'équipe de faux pirates informatiques, la *Red Team*, chargée de mener les attaques, n'était autorisée qu'à utiliser du matériel disponible dans le commerce et les informations disponibles sur le web, avec interdiction de violer la législation américaine.

A ce jour, les résultats de cet exercice demeurent strictement "top secret". De nombreux responsables y ont néanmoins fait allusion dans des déclarations publiques et certains d'entre eux ont même partiellement levé le voile sur les résultats. Un journaliste qui travaille à Washington affirme dans un livre avoir interviewé de hauts responsables à propos de *Eligible Receiver* : "Les attaques [simulées] ont été concentrées contre trois cibles principales : l'infrastructure d'information nationale, le commandement militaire et le pouvoir politique. Dans chaque cas, les 'pirates' n'ont éprouvé aucune difficulté à s'introduire dans des systèmes apparemment bien protégés. Les systèmes de contrôle du trafic aérien ont été mis hors service, une panne d'électricité généralisée a été provoquée, le pompage alimentant les raffineries de pétrole a été interrompu, à chaque fois à la suite, apparemment, d'incidents fortuits. Parallèlement, pour répondre à une crise internationale imaginaire, le département de la Défense procédait à un déploiement de forces à l'étranger et le réseau logistique entrait en action. Il s'est avéré remarquablement simple de perturber ce réseau en modifiant les ordres [...] et en interrompant le flux logistique [...]. Les "pirates" ont commencé à introduire des bulletins d'information erronés dans le processus de prise de décision, de sorte que les politiciens se sont retrouvés confrontés à un refus par l'opinion publique de voir participer les Etats-Unis à un conflit potentiel, tout en ne disposant pas d'informations détaillées et précises [...]."

Ainsi, il apparaît qu'une équipe de pirates informatiques expérimentés, utilisant un équipement standard et des informations du domaine public tout en respectant les limites légales, est parvenue à provoquer une "sérieuse dégradation de l'aptitude du Pentagone à procéder à un déploiement et à combattre". En d'autres termes, cette équipe a fait la preuve qu'un "Pearl Harbor électronique" était possible.

Depuis lors, de nombreux pays déploient des efforts pour faire face à la menace d'attaques contre leurs systèmes d'information, ou de guerre de l'information. En règle générale, les conseillers de l'armée et de la défense ont été les premiers à s'intéresser à la question, mais la plupart des gouvernements occidentaux ont désormais pris des mesures en vue d'apporter des réponses plus coordonnées et structurées.

Aux **Etats-Unis**, plusieurs Comités, Commissions et Groupes d'étude examinent ces questions depuis le début des années '90 et le gouvernement a adopté diverses mesures importantes. Des commissions du Congrès organisent des

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

auditions pour enquêter sur la nature de la menace posée par la guerre de l'information.

L'évaluation la plus complète des faiblesses des Etats-Unis dans le domaine de la technologie informatique provient toutefois de la *Commission présidentielle pour la protection des infrastructures critiques*. Créée en 1996, elle a publié un rapport complet qui met en lumière les faiblesses de l'infrastructure américaine et la vulnérabilité des systèmes d'information, susceptibles de constituer une cible potentiellement facile de toute attaque concertée. Le rapport indique également que le gouvernement et l'industrie ne partagent pas efficacement leurs informations susceptibles d'avertir d'une attaque électronique, et que le budget fédéral de recherche et développement ne comporte pas de poste pour l'analyse des menaces pour les systèmes d'information.

Certains experts critiquent les décisions de l'administration américaine, faisant valoir que les dispositions que nous venons de citer sous-estiment les réalités de la menace posée par la guerre de l'information. Il n'en demeure pas moins qu'il s'agit là de l'initiative la plus complète adoptée à ce jour par un gouvernement occidental pour faire face aux risques d'attaques sur les systèmes d'information.

De son côté, le Département américain de la Défense, qui participe activement aux initiatives du gouvernement, a créé une *Force d'intervention conjointe pour la défense des réseaux informatiques* (JTF-CND), chargée de coordonner toutes les activités dans ce domaine et d'orienter la réponse du Pentagone en cas d'attaques contre les réseaux informatiques. Cette force d'intervention conjointe planifie les mesures défensives, tire parti des capacités existantes et développe des procédures pour les chefs d'état-major, les services et agences gouvernementaux. Elle veille en outre à ce que l'attention stratégique requise soit apportée à tous les échelons. La force d'intervention conjointe développe également des relations avec les services de renseignement et les agences chargées de l'application des lois, le NIPC et le secteur privé.

Parmi les pays européens, c'est la **France** qui semble avoir développé la stratégie la plus cohérente pour faire face à des attaques contre ses systèmes d'information. En l'absence d'un programme général pour la protection de l'infrastructure, comme celui existant aux Etats-Unis, la Délégation générale pour l'armement (DGA) du ministère de la Défense concentre ses activités techniques dans le domaine de la guerre de l'information au Centre d'électronique de l'armement (CELAR). Ce centre, qui rassemble environ 900 experts dans de nombreuses disciplines scientifiques et technologiques, dispose de ressources et de capacités probablement sans équivalent sur le continent européen. Toutes les activités du CELAR sont liées à la guerre de l'information, défensive et offensive, et se répartissent en cinq pôles : les systèmes d'armes pour la guerre électronique, la sécurité de l'information, les systèmes d'information, les télécommunications et les composants électroniques. Le CELAR analyse les menaces, définit les besoins et teste la capacité et les limites des systèmes et équipements. Dans le cadre de la mission dévolue au CELAR, le Centre de l'armement pour la sécurité des systèmes d'information (CASSI) est responsable de tous les programmes et stratégies de sécurité au ministère de la Défense et sert de consultant pour les autres ministères et les agences gouvernementales.

En **Allemagne**, les efforts du gouvernement et du Bundestag pour faire face au problème de la sécurité en technologie informatique ont conduit à la création, en 1991, d'une Agence fédérale pour la sécurité en technologie informatique (Bundesamt für Sicherheit in der Informationstechnik ou BSI). La BSI est chargée de l'évaluation des risques de l'élaboration des critères, outils et procédures destinés à assurer la sécurité des systèmes vitaux d'information. D'après des responsables allemands, la BSI concentre toutefois ses travaux sur les aspects non militaires de la guerre de l'information. En d'autres termes, elle envisage la possibilité d'attaques dans le domaine civil uniquement. L'armée allemande a parallèlement effectué plusieurs études sur la guerre de l'information et vient d'en entamer une nouvelle, appelée "2020", qui étudiera l'évolution future en la matière. Un groupe de travail a récemment été créé au niveau fédéral pour rédiger un document sur "La guerre de l'information et la sécurité informatique" dans le but de parvenir à une meilleure coordination au sein des domaines civils et militaires.

Le ministère **britannique** de la Défense s'attaque de diverses manières aux problèmes liés à la guerre de l'information, tout en reconnaissant que "les faiblesses et risques potentiels résultant de la guerre de l'information dépassent largement les infrastructures des forces armées et de la défense". Le ministère britannique de la Défense collabore en conséquence avec d'autres agences gouvernementales, des alliés et des fournisseurs de services essentiels afin de coordonner les politiques de sécurité et de trouver des solutions techniques pour protéger l'infrastructure nationale.

D'autres pays ont adopté des initiatives similaires. Pour sa part, l'**OTAN** analyse les menaces liées à des attaques menées dans le cadre de la guerre de l'information et fournit des indications aux Etats membres. Pour le moment, les études les plus pertinentes menées par l'Alliance sur ce thème ne peuvent être divulguées.

Comme c'est souvent le cas pour les questions faisant l'objet d'intenses débats, certains analystes de la défense et experts de la sécurité de l'information doutent de l'ampleur réelle de la menace liée à la guerre de l'information telle qu'elle est présentée par les médias et même par certains rapports officiels. Ils affirment que les journaux et les magazines déforment la réalité et exagèrent les intrusions au sein des sites web militaires et des systèmes d'information des sociétés.

Des spécialistes en informatique et des experts en sécurité informatique admettent que des gens mal intentionnés peuvent s'introduire dans des serveurs web civils et militaires, et qu'ils peuvent même occasionner de sérieux dommages, mais que tout cela est loin de représenter un "Pearl Harbor électronique" pour les Etats-Unis.

Pour ce qui concerne les résultats prétendument effrayants de l'exercice *Eligible Receiver*, les experts informatiques déclarent en outre que l'attitude du Pentagone contraste fortement avec le caractère largement ouvert des discussions sur les faiblesses de la sécurité informatique qui prolifèrent sur Internet.

D'après le rédacteur en chef de *US Military Online*, l'excessive discrétion du Pentagone quant à la sécurité de l'information reflète une erreur fondamentale d'interprétation de la puissance d'Internet et de la capacité des militaires à la

contrôler. Une directive publiée le 24 septembre 1998 par le secrétaire adjoint à la Défense, assurait tous les services et agences de l'armée que "la sécurité nationale n'est pas compromise, ni le personnel militaire soumis à des risques" en raison des informations disponibles sur les sites web militaires. En fait, le Pentagone a, pendant des années, mené des politiques assorties de telles exigences, ce qui explique que seules les informations non confidentielles soient publiées sur Internet.

De nombreux experts et scientifiques critiquent les politiques du gouvernement, non pas parce qu'ils pensent que le cyberespace ne peut pas être une source de menaces, mais parce qu'ils estiment que ces menaces ont sans doute été exagérées ou mystifiées par une rhétorique formulée par des "guerriers de l'information" comme ils les qualifient.

Des analystes en sécurité informatique, qui ont étudié ces problèmes depuis des années, ont l'impression que "la guerre de l'information" est le même vieux problème sous une apparence nouvelle. En réalité, nombre des activités tombant actuellement sous cette définition pourraient s'avérer être des opérations relevant du "renseignement" traditionnel, d'analyses du renseignement via Internet ou d'opérations ou leurres psychologiques. L'*US Air Force Information Warfare Center* (AFIWC, qui fait partie de l'*Air Intelligence Agency*), basée à San Antonio par exemple, ainsi que d'autres organismes similaires, sont l'équivalent d'équipes informatiques d'urgence, et les militaires et civils employés dans ces organisations sont tous des spécialistes de la sécurité informatique.

Selon le *The Crypt Newsletter*, une publication Internet américaine qui traite de la sécurité informatique et s'adresse aux analystes informatiques : "Il est loin d'être prouvé que le pays est à la merci d'attaques informatisées potentiellement dévastatrices. D'autre part, même le petit nombre d'exemples de comportements pervers atteste que les problèmes de sécurité informatique dans notre monde de plus en plus technologique constituera l'une des préoccupations majeures dans un proche avenir."

Il ne fait aucun doute que, même si l'on s'en réfère aux déclarations des analystes les plus sceptiques, la sécurité des systèmes d'information doit figurer parmi les priorités les plus élevées d'une nation. Face à la dépendance croissante à l'égard des technologies de l'information, toutes nos infrastructures vitales sont potentiellement vulnérables à l'une ou l'autre forme d'attaque externe. Même si les experts ne sont pas d'accord quant à la portée et à la nature de la menace, nos responsables doivent néanmoins adopter des mesures pour renforcer la protection de nos systèmes d'information.

La première priorité devrait porter sur la recherche de l'objectivité dans toute évaluation des menaces réelles. Il y aurait lieu de constituer un groupe indépendant chargé de procéder à ces évaluations, probablement au niveau international. Les parlements et les gouvernements, ainsi que l'industrie, les milieux scientifiques et les spécialistes de la sécurité informatique devraient être représentés au sein de ce groupe afin de partager leurs connaissances et leurs compétences et d'analyser la problématique sous différents angles. Leur première mission pourrait être l'évaluation sérieuse des revendications formulées par les constructeurs de matériels et les éditeurs de logiciels de sécurité.

La législation doit suivre le développement de nouvelles technologies. Les parlements peuvent jouer un rôle important pour revoir et amender les lois régissant la protection des infrastructures et la sécurité des systèmes d'information. Cet effort de révision par le législateur devrait être entrepris aussi bien au niveau local, que national et international.

Les cellules de renseignement peuvent, elles aussi, aider à mieux comprendre les nouvelles menaces liées à l'ère de l'information, en termes d'acteurs, de motifs et de capacités. Bien sûr, le travail et l'organisation du renseignement traditionnel, développés pendant la Guerre froide, doivent être adaptés au nouvel environnement. Les responsables du renseignement dans tous les Etats doivent reconsidérer leurs méthodes d'acquisition de l'information et se fier à de nouvelles sources. Les agences nationales doivent également commencer à recruter des spécialistes, parfaitement au fait des nouvelles menaces (par exemple des analystes informatiques compétents ayant une expérience directe des méthodes de craquage).

Comme la plupart des experts s'accordent à reconnaître que les systèmes d'information commerciaux sont aujourd'hui plus vulnérables aux attaques externes, il est essentiel de promouvoir la coopération entre secteur privé et secteur public. La plupart des informations dont les sociétés privées ont besoin pour protéger leurs systèmes d'information peuvent être mises à disposition par les milieux de la défense, du renseignement et des autorités chargées de faire respecter la loi. Il arrive souvent que le secteur privé puisse mieux identifier, comprendre et évaluer les menaces. Dans de nombreux pays, la collaboration entre l'industrie et les instances publiques pourrait s'avérer extrêmement utile pour partager "l'information et les techniques se rapportant à l'évaluation de la gestion des risques, y compris les comptes-rendus d'incidents, l'identification des points faibles, les plans et la technologie visant à prévenir les attaques et interruptions, et les plans de restauration en cas de sinistre". Il va de soi que la collaboration entre secteur privé et secteur public a également ses limites, sous la forme notamment d'informations secrètes et confidentielles ou "déposées" ou sensibles d'un point de vue concurrentiel.

Enfin, dans la plupart des pays occidentaux, mais surtout aux Etats-Unis, les militaires devraient aborder plusieurs questions relatives au rôle effectif des programmes de guerre de l'information dans leur politique générale.

Le lien entre la guerre de l'information et d'autres stratégies militaires devrait être plus clairement formulé : par exemple, serait-il envisageable de riposter avec des armes conventionnelles à une attaque relevant de la guerre de l'information ? De plus, la possibilité que les Etats-Unis (ou tout autre pays occidental) développent et déploient des techniques offensives de guerre de l'information n'a pas été débattue de façon appropriée dans les enceintes publiques. Ce débat pourrait s'avérer essentiel si l'on veut parvenir à un consensus national et si possible international à propos du rôle de la guerre de l'information offensive et définir clairement ses règles d'utilisation.

Cette menace crée-t-elle ainsi de nouvelles fonctions ou bien est-ce l’inverse ?

Lt (R) Paul SCIMAR