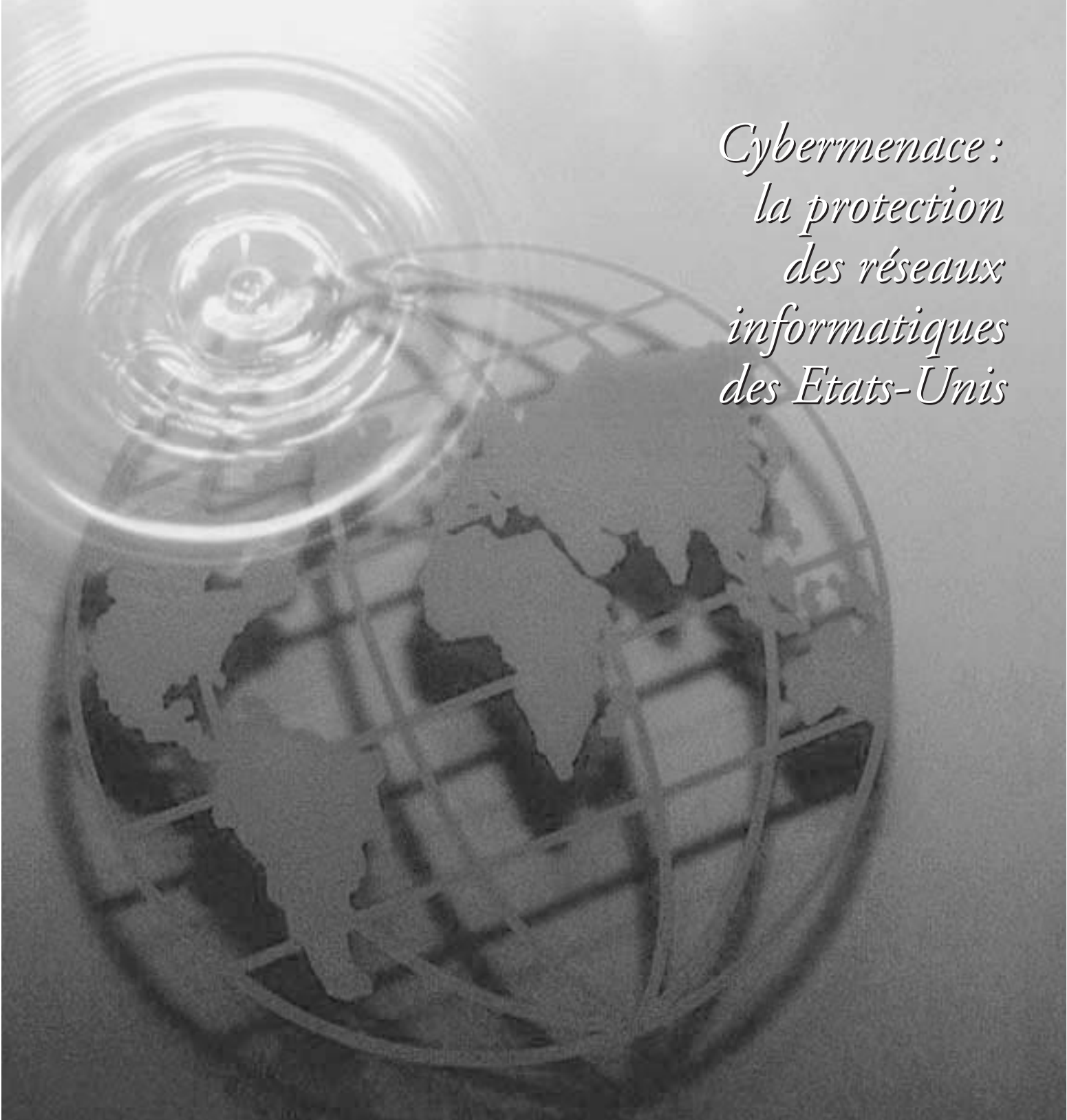

LES OBJECTIFS DE POLITIQUE ETRANGERE DES ETATS-UNIS

VOLUME 3

REVUE ELECTRONIQUE DE L'AGENCE D'INFORMATION DES ETATS-UNIS

NUMERO 4



*Cybermenace:
la protection
des réseaux
informatiques
des Etats-Unis*

Novembre 1998

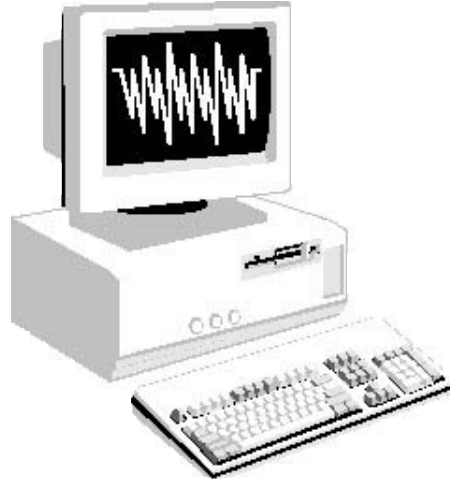
LES OBJECTIFS DE POLITIQUE ETRANGERE DES ETATS-UNIS

Cybermenace : la protection des réseaux informatiques des Etats-Unis

LES OBJECTIFS DE POLITIQUE ETRANGERE DES ETATS-UNIS

REVUE ELECTRONIQUE DE L'USIA

VOLUME 3 • NUMERO 4 • NOVEMBRE 1998



« A l'aube du XXI^e siècle, nos ennemis élargissent le champ de bataille de l'espace physique au cyberspace (...) Au lieu de débarquer sur nos plages ou de lancer leurs bombardiers, ces adversaires pourraient diriger des cyberattaques contre nos systèmes militaires essentiels ou contre notre infrastructure économique (...) Si nous voulons que nos enfants grandissent dans la sécurité et dans la liberté, nous devons faire face à ces nouveaux dangers du XXI^e siècle avec la même rigueur et la même détermination que nous avons mises à affronter en ce siècle-ci les menaces les plus graves faites à notre sécurité. »

Le président Clinton
Cérémonie de remise des diplômes de l'Académie navale,
22 mai 1998

Le présent numéro des « Objectifs de politique étrangère des Etats-Unis » examine les actions engagées par les Etats-Unis face aux défis tout nouveaux de l'âge de l'information. De hauts responsables gouvernementaux font le point des initiatives destinées à protéger les réseaux informatiques américains contre les tentatives de sabotage et à stimuler la coopération entre les secteurs public et privé en vue de la mise en place de dispositifs de sécurité. Par ailleurs, un sénateur fédéral présente la réaction du Congrès au débat sur la cyberguerre ; un universitaire traite de la manière dont les établissements d'enseignement supérieur répondent aux nouvelles priorités nationales ; un spécialiste du secteur privé brosse un tableau général des enjeux et de l'évolution de la cyberguerre ; enfin, des responsables du secteur privé spécialisés dans la sécurité de l'information décrivent la collaboration que les entreprises privées des Etats-Unis ont forgée entre elles et avec le secteur public afin de satisfaire aux impératifs de sécurité de cette ère nouvelle.

LES OBJECTIFS DE POLITIQUE ETRANGERE DES ETATS-UNIS

*Revue électronique de l'Agence
d'information des Etats-Unis*

CYBERMENACE : LA PROTECTION DES RESEAUX INFORMATIQUES DES ETATS-UNIS

SOMMAIRE

● DOSSIER

DEFENDRE LA NATION CONTRE LES CYBERATTAQUES :

LA SECURITE DE L'INFORMATION DANS L'ENVIRONNEMENT MONDIAL 5

*Le général Kenneth Minihan
Directeur de l'Agence de la sécurité nationale*

LA PROTECTION DE L'INFORMATION ET LA NOUVELLE ERE DE LA SECURITE 9

*John Hamre
Secrétaire adjoint à la Défense*

CIAO : UNE STRATEGIE INTEGREE FACE AUX MENACES D'UNE ERE NOUVELLE 12

*Entretien avec M. Jeffrey Hunker
Directeur du Bureau de la protection de l'infrastructure critique*

LE PROBLEME DE L'AN 2000 17

*John Koskinen
Président du Conseil présidentiel sur le passage informatique à l'an 2000*

LA MENACE DE CYBERGUERRE APPELLE TOUS LES SECTEURS A UNE VIGILANCE ACCRUE 19

Entretien avec le sénateur Jon Kyl

● ANALYSE

DES FANTOMES DANS LES ORDINATEURS ? 23

*Martin Libicki
Directeur du bureau d'analyses à la société RAND*

LA REPOSE DE L'ENSEIGNEMENT SUPERIEUR A LA GUERRE INFORMATIQUE 28

*Charles Reynolds
Directeur du département d'informatique et doyen intérimaire de la Faculté des sciences et technologies
intégrées de l'université James Madison*

● L'OPINION DU SECTEUR PRIVE

LES SECTEURS PUBLIC ET PRIVE ONT INTERET A PARTAGER LEUR EXPERTISE DANS LE DOMAINE DE LA SECURITE 33

Entretien avec M. Howard Schmidt, directeur de la sécurité informatique chez Microsoft

ASSURER LA SECURITE DES SYSTEMES INFORMATIQUES 36

*James Lingerfeldt
Consultant principal chez IBM pour la sécurité publique et les affaires judiciaires*

James Adams
Président-directeur général d'« Infrastructure Defense, Inc. »

© DOCUMENT

FICHE DOCUMENTAIRE: LA PROTECTION DE L'INFRASTRUCTURE DE BASE DES ETATS-UNIS 46

Décret présidentiel 63

© RUBRIQUES

ARTICLES RECENTS 48

(En anglais)

BIBLIOGRAPHIE 49

(En anglais)

SITES INTERNET 50

(En anglais)

LES OBJECTIFS DE POLITIQUE ETRANGERE DES ETATS-UNIS

REVUE ELECTRONIQUE DE L'AGENCE D'INFORMATION DES ETATS-UNIS

VOLUME 3 • NUMERO 4 • NOVEMBRE 1998

Les revues électroniques diffusées à intervalle de trois semaines par l'USIA dans le monde entier examinent les principales questions d'actualité intéressant la communauté internationale. Dans cinq numéros distincts Perspectives économiques, Dossiers mondiaux, Démocratie et droits de l'homme, Les Objectifs de politique étrangère des États-Unis et La Société américaine elles présentent des articles de fond, des analyses, des commentaires et des renseignements de base sur un thème donné. Toutes les revues sont publiées en anglais, en français et en espagnol, et certains numéros sont traduits également en arabe, en portugais et en russe.

Les opinions qui sont exprimées dans les revues ne représentent pas nécessairement le point de vue du gouvernement des États-Unis. Veuillez noter que l'USIA n'est nullement responsable du contenu ou de l'accessibilité des sites Internet indiqués en hyperlien. Les articles de ces revues peuvent être librement reproduits en dehors des États-Unis, sauf indication contraire.

Les numéros les plus récents ainsi que les archives sont disponibles sur Internet à la page d'accueil des revues du Service d'information des États-Unis (USIS), à l'adresse suivante: <http://www.usia.gov/journals/journals.htm>

Veuillez adresser toute correspondance soit à votre centre local de l'USIS, soit à la rédaction:

*Editor, U.S. Foreign Policy Agenda
 Political Security I/TPS
 U.S. Information Agency
 301 4th Street, S.W.
 Washington, D.C. 20547
 États Unis d'Amérique
 Courrier électronique: ejforpol@usia.gov*

Veuillez noter que ce numéro des « Objectifs de politique étrangère des États-Unis » figure à la page d'accueil du Service d'information des États-Unis (USIS) à l'adresse suivante:

« <http://www.usia.gov/journals/itps/1198/ijpf/ijpf1198.htm> »

DIRECTEUR DE LA RÉDACTION Leslie High
 RÉDACTRICE EN CHEF Dian McDonald
 RÉDACTEURS EN CHEF ADJOINTS. . . Wayne Hall
 Guy Olson
 RÉDACTEURS. Ralph Dannheisser
 Susan Ellis
 Margaret McKay
 Jody Rose Platt
 Jacqui Porth
 RECHERCHE ET DOCUMENTATION . . Rebecca Ford Mitchell
 Vivian Stahl
 CONCEPTION GRAPHIQUE Barbara Long
 ASSISTANTE ARTISTIQUE Sylvia Scott
 TRADUCTION Services linguistiques
 de l'USIA
 CONSEIL DE RÉDACTION Howard Cincotta
 Rosemary Crockett
 John Davis Hamill

DEFENDRE LA NATION CONTRE LES CYBERATTAQUES : LA SECURITE DE L'INFORMATION DANS L'ENVIRONNEMENT MONDIAL

*By Lieutenant General Kenneth A. Minihan
Director, National Security Agency*

L'Agence de la sécurité nationale « fait appel à ses compétences spécialisées pour élaborer la technologie fondamentale qui établira des capacités nationales de détection des cyberattaques et de riposte à ces attaques », déclare le général de l'armée de l'air Kenneth Minihan. Il souligne que « la supériorité des moyens informatiques à l'âge de l'information est de toute évidence un impératif national ».

« NOUS SOMMES EXPOSÉS À DES RISQUES. LES ETATS-UNIS DÉPENDENT DES ORDINATEURS. CES DERNIERS CONTRÔLENT L'ALIMENTATION EN ÉNERGIE, LES COMMUNICATIONS, L'AVIATION ET LES SERVICES FINANCIERS. ILS SERVENT À ARCHIVER DES INFORMATIONS VITALES, TELLES QUE LES DOSSIERS MÉDICAUX, LES PLANS COMMERCIAUX ET LES CASIERS JUDICIAIRES. MALGRÉ LA CONFIANCE QUE NOUS LEUR FAISONS, ILS SONT VULNÉRABLES : VULNÉRABLES AUX DÉFAUTS DE CONCEPTION ET À L'INSUFFISANCE DU CONTRÔLE DE LA QUALITÉ, VULNÉRABLES AUX ACCIDENTS ET, PEUT ÊTRE EST-CE LÀ LE POINT LE PLUS ALARMANT, VULNÉRABLES AUX ATTAQUES INTENTIONNELLES. LE BRIGAND MODERNE PEUT VOLER DAVANTAGE MUNI D'UN ORDINATEUR QUE D'UNE ARME. LE TERRORISTE DE DEMAIN SERA PEUT-ÊTRE CAPABLE D'INFLIGER PLUS DE DOMMAGES À PARTIR D'UN CLAVIER QU'AU MOYEN D'UNE BOMBE. »

« Les ordinateurs en danger », Conseil national de la recherche, 1991

INTRODUCTION

L'aspect le plus remarquable de la citation qui précède est peut être qu'elle a été écrite pratiquement à l'aube de l'âge de l'information. Jusqu'à une date récente, nous n'avons guère prêté attention à la question. Les Etats-Unis, et le reste du monde, poursuivent leur progression dans la révolution de l'information ; la technologie de l'information s'infiltré chaque jour davantage dans la trame même de notre société et de notre économie en tant que pays membre de la

communauté mondiale. L'autoroute de l'information véhicule aujourd'hui, de manière très réelle, les principes vitaux de l'économie de notre pays.

S'ils sont à l'avant garde mondiale de l'âge de l'information, les Etats-Unis sont aussi devenus particulièrement tributaires des techniques de l'information, des ordinateurs et des réseaux mondiaux qui les relient. Cette dépendance évidente nous expose à de graves menaces qui pèsent sur notre bien être économique, notre sécurité publique et notre sécurité nationale.

Les réseaux mondiaux, communément décrits comme constituant le « cyberspace », ne connaissent pas de frontières physiques. Notre interconnexion croissante dans le cyberspace accroît notre vulnérabilité à nos ennemis traditionnels et à un groupe grandissant de nouveaux adversaires. Les terroristes, les groupes radicaux, les trafiquants de drogues et les associations de malfaiteurs se joindront aux Etats ennemis pour utiliser une panoplie toute nouvelle d'instruments informatiques sophistiqués d'agression. Les attaques informatiques peuvent compléter ou remplacer les attaques militaires traditionnelles, accroître considérablement notre vulnérabilité et compliquer d'autant les parades à prévoir et à mettre en place. Les ressources exposées à ces dangers comprennent non seulement l'information emmagasinée ou véhiculée dans le cyberspace, mais aussi toutes les composantes de notre infrastructure nationale qui dépendent de la technologie de l'information et de la disponibilité en temps voulu de données exactes. Parmi ces composantes figurent l'infrastructure des télécommunications elle même, nos systèmes bancaires

et financiers, les réseaux d'énergie électrique, les autres éléments d'infrastructure énergétique tels que les oléoducs et les gazoducs, nos réseaux de transport, les systèmes d'alimentation en eau, les systèmes de soins médicaux et de santé, les services d'urgence tels que la police, les pompiers et les opérations de sauvetage, et les activités gouvernementales à tous les niveaux. Tous ces éléments sont nécessaires au succès économique et à la sécurité de la nation.

LA PROTECTION DE L'INFORMATION : L'OBJECTIF NATIONAL

Le 22 mai 1998, le président a signé le Décret présidentiel 63 (PDD 63) sur la protection de l'infrastructure critique. Son objectif, déclaré dans le texte, est le suivant : « J'entends que les Etats-Unis prennent les mesures nécessaires pour éliminer promptement tout point vulnérable important qui exposerait leurs éléments d'infrastructure essentiels, notamment leurs systèmes informatiques, aux attaques cybernétiques comme physiques.

L'objectif national est qu'au plus tard en l'an 2000, les Etats-Unis se soient dotés d'une capacité opérationnelle de départ et que dans les cinq ans à dater de ce jour, la nation soit en mesure de protéger ses éléments d'infrastructure essentiels des actes intentionnels qui porteraient une atteinte significative à la capacité :

- du gouvernement fédéral de s'acquitter des missions essentielles à la sécurité nationale et d'assurer la santé et l'ordre publics,
- des gouvernements locaux de maintenir l'ordre et de fournir les services publics essentiels à un niveau minimum,
- du secteur privé d'assurer le bon fonctionnement de l'économie et de fournir les services essentiels de télécommunications, d'énergie, de finances et de transports. »

La réalisation d'un objectif d'une telle ampleur est une entreprise considérable, qui exigera des efforts coopératifs entre le gouvernement et les entités du secteur privé qui gèrent les éléments vitaux de l'infrastructure. Le décret présidentiel charge le gouvernement fédéral de donner l'exemple en assurant la solidité des systèmes fédéraux, tout en précisant clairement que le secteur public ne saurait résoudre ce problème de manière unilatérale. Chacun des services et

des organismes fédéraux est fortement tributaire des services fournis par le secteur privé : énergie, télécommunications, transports, etc. En conséquence, le décret envisage un partenariat public privé pour élaborer et mettre en application un plan exhaustif de protection de l'infrastructure nationale, pour parer aux menaces du terrorisme électronique. La principale difficulté consistera à amener le secteur privé à envisager la protection de l'infrastructure dans une optique nationale. Dans l'environnement actuel hautement concurrentiel, le secteur privé vise normalement à s'assurer des avantages sur le marché, notamment en maîtrisant ses coûts d'exploitation, afin de maximiser ses bénéfices. Or le renforcement des mesures de cyberprotection exigera une augmentation des investissements et un élargissement de la coopération avec les concurrents.

COMPOSANTES STRATÉGIQUES ESSENTIELLES

Toute stratégie visant au renforcement des éléments vitaux de notre infrastructure doit comprendre trois composantes fondamentales : protection accrue contre les attaques cybernétiques ; capacité de détecter les attaques au moment où elles se produisent ; capacité de riposte ou de reprise des activités une fois que l'attaque a été détectée.

Le renforcement de la protection contre les cyberattaques se fonde sur la technologie du cryptage, notamment les signatures numérisées, afin de fournir les services d'authentification, de vérification d'intégrité, de non répudiation, et de confidentialité nécessaires. Un dispositif performant d'authentification à base de signature numérique utilisé pour contrôler l'accès est peut être la parade la plus puissante contre une attaque cybernétique. La signature numérique permet également d'assurer l'intégrité de l'information électronique et la non répudiation des transactions cybernétiques. Le cryptage est appliqué aux ordinateurs personnels, aux serveurs de fichiers et aux réseaux pour assurer la confidentialité des informations sensibles tant gouvernementales que commerciales et personnelles. Cette technologie, naguère presque exclusivement réservée au secteur public, mais aujourd'hui largement disponible sur le marché commercial, est un élément fondamental de la mise en œuvre des stratégies de protection de l'information. En fait, le 16 septembre

1998, le vice président a annoncé une importante révision de la réglementation des exportations des Etats-Unis concernant les techniques de cryptage, ce qui indique clairement toute l'importance qu'elles revêtent pour la protection de l'infrastructure vitale ainsi que pour le commerce électronique mondial et la prospérité économique.

Etant donné le stade avancé de développement de la technologie du cryptage, le défi qui reste consiste à l'appliquer de manière cohérente et efficace pour protéger tous les éléments d'infrastructure essentiels. Cela exige un cadre d'application adaptable à différentes échelles et interopérable, accompagné d'un système public de clés (SPC) de cryptage destiné à fournir des signatures numériques robustes et mondialement reconnaissables et des certificats de clés de cryptage, « l'identification électronique » individuelle unique de l'âge de l'information. Les services de SPC commencent à se développer dans le secteur privé pour satisfaire la demande du commerce électronique mondial et ils pourraient être mis à contribution pour appuyer la protection de l'infrastructure vitale.

En revanche, face aux cyberattaques, les techniques de diagnostic, de détection et de riposte ne sont encore ni très avancées ni très efficaces. Les Etats-Unis ont des capacités très limitées lorsqu'il s'agit d'identifier ou de reconnaître une attaque cybernétique lancée contre le gouvernement ou contre l'infrastructure du secteur privé, et leur capacité de riposte est encore plus faible. Or la capacité d'identifier une cyberattaque stratégique visant un ou plusieurs éléments vitaux d'infrastructure et d'y réagir de manière appropriée est à l'évidence une question primordiale de sécurité nationale. L'un des facteurs qui compliquent la situation est que les atteintes à l'intégrité des systèmes informatiques ont jusqu'ici été considérées comme des actes criminels, relevant des compétences des forces de police. Lorsqu'il s'est produit une intrusion, l'intrus (il faut l'espérer) a été retrouvé, arrêté et poursuivi. De plus, de nombreuses entités du secteur privé hésitent à partager les informations relatives à ces intrusions, craignant des articles défavorables dans la presse des gros titres du genre « Effraction dans les ordinateurs de la Banque X: les pertes se chiffrent dans les millions de dollars » ou « Des cyberpirates perturbent les réseaux téléphoniques » et les réactions du public qui en découleraient. Pour développer des capacités de défense

cybernétique efficaces au niveau national, de nouvelles règles d'engagement doivent être formulées afin de permettre une collaboration ouverte et dynamique entre le secteur privé, les forces de l'ordre et les responsables de la sécurité nationale.

LE NOUVEAU RÔLE DE L'AGENCE DE SÉCURITÉ NATIONALE EN MATIÈRE DE PROTECTION DE L'INFORMATION

A l'âge de l'information, les missions traditionnelles de renseignement et de sécurité des systèmes d'information de l'Agence de sécurité nationale (National Security Agency, NSA) évoluent et visent à assurer la supériorité de l'information aux Etats-Unis et à leurs alliés. Il faut pour cela une compréhension profonde de l'infrastructure de l'information mondiale et de la vulnérabilité des réseaux informatiques aux cyberattaques. Du côté défensif de la mission, la NSA a pris une série d'initiatives destinées à établir les fondations techniques de la protection de notre infrastructure vitale.

Comme je l'ai mentionné plus haut, la technologie du cryptage est aujourd'hui largement disponible sur le marché commercial et c'est sur elle que repose la protection des systèmes d'information contre les attaques cybernétiques. La mauvaise nouvelle est que les nombreux produits disponibles n'interopèrent pas de manière sûre et sont d'une robustesse variable, et qu'il existe de multiples manières, souvent contradictoires, de crypter l'information. C'est ainsi qu'il existe un cryptage de courrier électronique, un cryptage de fichier, un cryptage Internet, un cryptage de liaison, et un cryptage de réseau privé virtuel, pour ne citer que quelques unes de ces variations. Pour remédier à cette situation, la NSA a formé un partenariat avec les principaux fournisseurs de techniques de sécurité de l'information pour élaborer une matrice commune de services de cryptage afin d'offrir des solutions de protection de l'information au niveau de l'ensemble de l'entreprise. Cette matrice définit une manière cohérente d'appliquer la technologie du cryptage à l'entreprise, et précise la manière dont le cryptage se marie aux autres techniques et produits de sécurité et les renforce, par exemple les filtres sécuritaires, les serveurs, les routeurs, les systèmes d'exploitation, les détecteurs d'intrusions, les instruments de vérification des fichiers et les services de systèmes publics de clés.

Un autre aspect du problème est celui des degrés divers de robustesse des nombreux produits de sécurité disponibles sur le marché. Pour résoudre la question, la NSA s'est associée à l'Institut national des normes et de la technologie (NIST). Au titre de leur accord, la NSA et le NIST homologueront les laboratoires commerciaux qui évalueront la sécurité commerciale des produits considérés, soit pour valider les affirmations de sécurité des fournisseurs, soit pour déterminer la conformité des produits aux exigences du dispositif de sécurité du réseau. Les essais des produits seront effectués et vérifiés par les laboratoires homologués contre rémunération, les tarifs et les arrangements devant être négociés entre le laboratoire et le fournisseur du produit.

Enfin, la NSA considère que le pays a besoin d'un système partagé de dispositifs d'assurance de sécurité de l'information et elle fait appel à ses compétences spécialisées pour élaborer la technologie fondamentale qui établira des capacités nationales de détection des cyberattaques et de riposte à ces attaques. Ce système est doté d'une variété de capteurs qui peuvent être mis en place à des points essentiels de l'infrastructure et dans l'infrastructure de télécommunications sous jacente elle-même, à l'aide de techniques analytiques sophistiquées de grande envergure, pour fournir un aperçu dynamique des menaces cyberspatiales auxquelles sont exposés les éléments vitaux d'infrastructure. Ces techniques devraient être partagées par tout un ensemble d'entités de sécurité nationale, tant fédérales qu'industrielles et régionales, pour permettre en simultané les opérations de détection, de défense, de reconstitution et de reprise des services vitaux.

CONCLUSION

La prospérité économique dont jouit notre pays aujourd'hui se fonde largement sur l'âge de l'information et sur notre prééminence technologique mondiale dans ce domaine. Notre influence prépondérante sur l'économie mondiale et notre prospérité pourraient fort bien dépendre de notre volonté nationale de prendre l'initiative en vue d'instaurer l'intégrité et la responsabilité «l'assurance de l'information» dans l'environnement informatique mondial que nous avons contribué à créer. Par son Décret présidentiel 63, le gouvernement Clinton proclame qu'il est temps d'agir et la NSA est bien positionnée et prête à se charger de la mission, au service de laquelle elle mettra son savoir faire technique. La supériorité des moyens informatiques à l'âge de l'information est de toute évidence un impératif national. ©

LA PROTECTION DE L'INFORMATION ET LA NOUVELLE ÈRE DE LA SÉCURITÉ

John Hamre
Secrétaire adjoint à la Défense

La protection des ressources informatiques critiques sera l'un des grands défis qui se poseront à la sécurité des Etats-Unis au cours des années à venir, affirme le secrétaire adjoint à la Défense, M. John Hamre. Notant que le Pentagone est chargé de la protection de vingt huit mille réseaux informatiques, il estime que la protection du monde virtuel contre les « cybermenaces » est autant une question de gestion et de vigilance qu'un problème technique ».

Les Etats-Unis sont passés par cinq ères successives en matière de sécurité, chaque transition s'effectuant dans le sens d'un passé certain à un avenir incertain. La première a duré de la guerre d'Indépendance jusqu'au milieu des années 1820, époque à laquelle les Etats-Unis se trouvaient à la périphérie d'un environnement international toujours dominé par l'Europe.

Au cours de la deuxième période, du milieu des années 1830 à la fin du XIX^e siècle, profitant de l'isolement que nous assurait l'océan Atlantique, nous nous sommes occupés de nos propres affaires pendant que la vieille machine politique de l'Europe se désintégrait. Cette ère s'est achevée à la Première Guerre mondiale et à la naissance de l'Union soviétique. La troisième époque, de 1920 à 1946, a été marquée par une récession mondiale et par la montée du communisme international tandis que l'Europe s'effondrait. Ces événements ont déclenché une crise de la démocratie américaine et du système de la libre entreprise avec la Grande dépression, et les tensions dans le domaine de la sécurité internationale ont abouti à la Deuxième Guerre mondiale. L'époque la plus récente, celle de la Guerre froide, a été dominée par un monde bipolaire. Les Etats-Unis ont été le fer de lance, au sein de la communauté internationale, de la création d'institutions destinées à appuyer la reconstruction des économies européennes en ruines et à faire face à l'effondrement des empires du tiers monde dominés par la vieille Europe. Ils ont également assumé la direction de la résistance opposée par les nations du monde libre au communisme, jusqu'à l'effondrement de l'Union soviétique.

Nous sommes aujourd'hui parvenus à une phase de transition qui nous mènera à une nouvelle époque,

apparemment caractérisée par la réapparition de deux vieux dangers, le nationalisme et l'ethnicité. Une autre caractéristique de cette nouvelle époque est l'expansion des technologies créées à l'époque précédente, la dissolution du contrôle relatif à ces technologies et la montée spectaculaire de nouvelles capacités techniques extraordinaires, porteuses d'un potentiel sans précédent pour le bien comme pour le mal. Nous vivons aujourd'hui dans la hantise de « l'éparpillement nucléaire » et d'armes chimiques et biologiques tombant entre les mains de terroristes.

L'époque à venir présentera également le défi de la sécurité cybernétique. L'essor spectaculaire des techniques informatiques a eu un effet profond sur tous les secteurs de l'économie et du gouvernement des Etats-Unis. Il a alimenté une croissance économique étonnante, amélioré les communications de manière spectaculaire et permis aux entreprises américains de faire face à leurs concurrentes de façon plus efficace que jamais. Les Etats-Unis, et le monde, dépendent aujourd'hui de la technologie de l'information dans des domaines qui auraient été inimaginables il y a quelques années seulement.

Ceci n'est nulle part plus vrai que dans les forces armées américaines. Le ministère de la défense des Etats-Unis a recours à la technologie informatique pour révolutionner véritablement les affaires militaires, par la transmission et l'utilisation d'énormes quantités d'information pour fournir des renseignements plus sûrs, améliorer radicalement le commandement et le contrôle, gérer ses activités de manière plus rentable, et se doter de systèmes d'armement plus puissants. Cette révolution est vitale pour nous maintenir en état de

défendre les intérêts des Etats-Unis aujourd'hui et pour nous préparer à faire face aux menaces toujours changeantes dont est porteuse l'époque à venir.

La révolution informatique touche tous les domaines relevant du ministère de la défense, aussi bien sur le terrain que dans les QG. Nos troupes au niveau de la section seront bientôt dotées de systèmes de communications qui permettront aux commandants de connaître avec précision la position de chaque soldat individuel, son état et même son rythme cardiaque, c'est à dire d'avoir une connaissance quasi totale de la situation sur le champ de bataille. De leurs navires en mer, nos marins envoient du courrier électronique à leur famille après avoir utilisé une technologie analogue pour guider des missiles de croisière. Les pilotes tiennent compte à présent du facteur de « saturation des tâches » résultant du flot d'information qu'ils ont à leur disposition en vol.

Dans le domaine logistique, la technologie de l'information est utilisée pour relier le front aux lignes de ravitaillement. Nous visons à la mise en place de procédures d'acquisitions sans papier d'ici à la fin du siècle. Nous avons ouvert un bureau des programmes électroniques pour rationaliser les achats au niveau de l'unité militaire et utilisons à présent l'internet pour nous ravitailler dans les supermarchés électroniques où nous achetons de tout, depuis les crayons jusqu'aux vérins hydrauliques de commande. Nous nous servons de l'internet pour effectuer toute une gamme de transactions, depuis le paiement des déplacements jusqu'aux communications par satellite, et nous avons fait d'énormes progrès en publication électronique.

En bref, le ministère de la défense recourt à toute la puissance du microprocesseur pour mettre sur pied l'armée du XXIe siècle. Ce faisant, nous devons toutefois reconnaître aussi que les nouvelles techniques sont assorties de certains dangers. Celles là mêmes qui nous permettent d'accroître notre efficacité peuvent également être utilisées par un ennemi qui, incapable de nous attaquer sur un champ de bataille classique, peut nous attaquer dans le cyberspace. Il y a là un aspect tout nouveau et très important de la théorie stratégique relative à la sécurité nationale : les techniques et moyens qui à une époque n'étaient accessibles qu'à de grands Etats sont désormais à la portée des particuliers. La protection de nos ressources

d'information, la sécurité de l'information, sera donc l'un des défis par lesquels la sécurité nationale se définira au cours des années à venir.

L'importance critique de la sécurité de l'information est très généralement reconnue. Au ministère de la défense, nous avons vu déferler la première vague de menaces cybernétiques dans le cadre d'un exercice d'une part et lors d'attaques réelles d'autre part. Pour déterminer dans quelle mesure nous étions vulnérables, nous avons procédé l'an dernier à un exercice. Notre « ennemi » était un groupe d'environ trente cinq personnes qui avaient pour mission de pénétrer les réseaux informatiques du ministère. Leurs instruments étaient limités à ceux qui se trouvent dans le commerce, aux techniques et aux logiciels standard vendus au détail ou téléchargeables par l'internet. En l'espace de trois mois, opérant dans le cadre de ces restrictions, le groupe a été en mesure de nous attaquer, d'accéder à nos réseaux non classés et, en fait, il aurait pu gravement perturber notre alimentation en électricité et nos systèmes de communications.

En février dernier, les réseaux du Pentagone ont été la cible d'une attaque organisée à un moment où nous intensifions notre déploiement dans le golfe Persique. Il s'est révélé que c'était l'œuvre de deux adolescents californiens, mais, survenant à un moment sensible comme elle l'a fait, cette attaque aurait pu être beaucoup plus grave. Notre exercice et les attaques de petite envergure que nous avons subies nous ont servi d'avertissement : il ne s'agissait plus de savoir si des attaques plus graves risquaient, oui ou non, d'être lancées contre nous, mais bien plutôt quand elles le seraient et où.

Pour parer à ces menaces, nous devons tout d'abord considérer nos idées préconçues. Les Américains ont traditionnellement conçu la sécurité en termes de barrières autour d'un enclos, de délimitation de frontières et de protection de la zone ainsi définie. En cas de brèche dans la barrière, elle peut être réparée et la sécurité est rétablie. Cette manière de voir était efficace lors des époques précédentes, mais il n'existe pas de frontières dans l'espace cybernétique. La transition qui mène à cette nouvelle époque doit être marquée non seulement par le progrès technique, ainsi aussi par une souplesse de pensée. Nous devons réaliser que la sécurité du monde virtuel est autant une question de gestion et de vigilance qu'un problème technique.

Modifier notre attitude est un exercice qui peut présenter de grandes difficultés. Sans nous en rendre compte, par exemple, nous fournissons actuellement à des ennemis en puissance des informations qu'ils avaient essayé d'acquérir précédemment moyennant des centaines de millions de dollars de dépenses. Nous avons une installation militaire qui possédait ce qui était considéré comme une excellente page d'accueil sur le Web. Elle montrait une vue aérienne du complexe, où les bâtiments étaient identifiés par des légendes : « Centre opérationnel » et « Centre d'appui technique ». C'était là un excellent instrument de relations publiques, mais il donnait également des renseignements précieux qui permettraient à ceux qui nous veulent du mal de cibler leur attaque.

Comprenant bien les grandes questions relatives à la sécurité de l'information, nous devons dans un second temps prendre des mesures concrètes pour protéger nos ressources informatiques. L'année dernière, le ministère de la défense a regroupé des initiatives disparates pour s'efforcer de cerner avec précision les exigences de protection de notre infrastructure de l'information. Le rythme des progrès techniques accroît d'autant l'ampleur de la tâche ; le ministère de la défense a vingt huit mille systèmes informatiques différents, tous en cours d'amélioration et de modification, et dont il faut évaluer la vulnérabilité. Assurer la sécurité de l'information est une tâche qui présente des analogies avec la guerre, et nous l'avons abordée dans cette optique en nommant un commandant des groupes de travail interarmes pour la défense des réseaux informatiques afin d'organiser nos efforts. Le ministère apporte également des contributions essentielles au Centre national de protection de l'information et au Bureau d'assurance de l'information critique du Président.

D'autres mesures sont aussi nécessaires. Quatre vingt dix pour cent de nos télécommunications se font actuellement par le réseau téléphonique public, ce qui fait du cryptage un élément central de la protection de l'information. L'un des dangers les plus graves, dans le monde virtuel, est que nos combattants reçoivent des messages « contrefaits » qui les induiront en erreur, si bien que sans cryptage valable, toute l'infrastructure de l'information dont nous dépendons est vulnérable. Pour parer à cette menace, nous cherchons actuellement au sein du ministère de la défense des moyens de garantir l'identité numérisée des utilisateurs et de développer un système cryptographique à clés publiques fiable. Nous devons renforcer nos processus de cryptage afin que les informations que nous transmettons et que nous exploitons par la voie électronique soient sécurisées et vérifiables.

Le ministère de la défense fait également des progrès notables en matière de sécurité générale des réseaux. Nous mettons en place des dispositifs de surveillance des réseaux et nous efforçons d'assurer le contrôle de la configuration dans cet environnement intrinsèquement changeant et dynamique des réseaux. Nous sommes en train d'installer des filtres sécuritaires, des centres de surveillance des réseaux, des signatures numériques et une infrastructure pour la sécurité.

La protection de l'information, le cryptage et la sécurité des réseaux soulèvent certains des problèmes les plus difficiles que le ministère de la défense ait jamais eu à résoudre. Pour bénéficier de la révolution informatique, nous devons assurer l'accès et la protection des avoirs dont nous dépendons. Nous progressons à pas de géants dans ce sens, mais il reste encore beaucoup à faire. Les défis du présent exigent que nous nous tournions vers les spécialistes de l'information, tant au ministère de la défense que dans l'ensemble des secteurs public et privé, pour protéger des systèmes auxquels nous attachons une importance vitale. Nous devons nous assurer que la voie dans laquelle notre nation s'engage pour accéder à la nouvelle ère de sécurité offre les mêmes garanties de succès que celle qu'elle a empruntée durant l'époque qui s'achève. ●

CIAO : UNE STRATEGIE INTEGREE FACE AUX MENACES D'UNE ERE NOUVELLE

*Entretien avec M. Jeffrey Hunker
Directeur du Bureau de la protection de l'infrastructure de base*

« Le soutien total du secteur privé » est indispensable pour mettre les infrastructures de base des Etats-Unis à l'abri d'une attaque dirigée contre leurs réseaux informatiques, déclare M. Jeffrey Hunker, directeur du Critical Infrastructure Assurance Office, ou CIAO, Bureau chargé de la protection des infrastructures clés. « La menace qui pèse sur nous ne fait que croître. C'est pourquoi nous devons réagir d'urgence et obtenir très rapidement des résultats pour la combattre », dit-il. M. Hunker était interviewé par Susan Ellis, collaboratrice régulière de la rédaction.

QUESTION : En tant que directeur du CIAO, vous avez pour tâche de mettre sur pied un plan national intégré contre les menaces physiques et cybernétiques qui pèsent sur les réseaux de communication, de transports, d'énergie et autres infrastructures de base. Quelle est la principale difficulté à laquelle vous vous heurtez en vous acquittant de vos nouvelles responsabilités découlant de l'initiative annoncée en mai dernier par le président Clinton ?

M. HUNKER : La principale difficulté mentionnée par le président est le fait que nous vivons actuellement dans une nouvelle ère sur laquelle pèsent des menaces jusque là inconnues. Nous vivons à une époque où, en raison de l'étroite interconnexion des télécommunications et d'Internet au réseau électrique, à nos principaux réseaux de transport, ces systèmes sont vulnérables à ce que nous appelons une attaque cybernétique, à l'utilisation par des pirates d'ordinateurs et d'Internet pour s'introduire dans ces systèmes et les perturber, les rendre inopérants. Une telle attaque risquerait d'entraver non seulement des opérations militaires, mais tous les services essentiels dont dépend notre économie et sur lesquels comptent les Américains l'électricité, le téléphone, les services de transports de base.

C'est un problème complètement nouveau qui s'est développé en raison de la technologie, des liens établis entre les divers secteurs de l'économie américaine. Notre principal problème consiste à renseigner le public sur cette nouvelle menace et à collaborer avec le secteur privé, les principales industries, pour obtenir les moyens de nous protéger contre ce type d'attaque cybernétique.

Q : C'est un phénomène complètement nouveau, n'est-ce pas ?

M. HUNKER : En effet. Nous avons réussi, au cours des dix dernières années, à interconnecter les divers secteurs économiques du pays et cela nous a valu d'importants avantages sur le plan de la croissance économique et du genre de prospérité dont jouissent les Etats-Unis. Mais cette nouvelle prospérité s'accompagne d'une vulnérabilité nouvelle et que ce soient des pays, des groupes terroristes ou des associations de malfaiteurs qui nous veuillent du mal, cette nouvelle vulnérabilité qui découle de notre dépendance à l'égard de systèmes électroniques et informatiques nous expose à des attaques d'un genre nouveau.

Q : Quelles sont les agences gouvernementales qui participent aux efforts déployés pour contrecarrer cette menace et comment votre bureau collabore-t-il avec elles pour s'acquitter de sa mission ?

M. HUNKER : Onze principales agences fédérales ont été chargées de cette tâche par le président. Ce sont notamment le ministère de la défense et les agences qui en dépendent ; les services chargés du renseignement et la police judiciaire, c'est à dire le Bureau fédéral d'enquête (FBI), le Service secret et le ministère de la justice. Il y a également les ministères du commerce, des finances et des transports. Tous ont reçu pour instruction de participer à l'établissement d'un plan national dans ce domaine.

Chose plus importante encore, on leur a demandé de s'associer au secteur privé. En effet, pratiquement toutes les infrastructures clés qui sont vulnérables à une

attaque appartiennent au secteur privé. Et si nous ne bénéficions pas de la coopération et du soutien complet du secteur privé dans l'acquisition de ces moyens de protection, nous n'irons pas très loin.

Q : Comment allez vous mesurer le succès de votre mission ?

M. HUNKER : Ce ne sera pas facile. Parce qu'il s'agit d'un problème nouveau et parce qu'à bien des égards, le type d'attaque et les menaces contre lesquels le président nous a demandé de protéger le pays sont en cours de développement, donc réellement nouveaux. Dans certains cas, ces menaces ne se sont pas encore matérialisées et notre succès va être difficile à mesurer. Je crois que l'un des principaux moyens d'y parvenir sera la mesure dans laquelle le secteur privé, les propriétaires et exploitants du réseau électrique et nos secteurs des transports, de la banque et des finances s'associeront au gouvernement pour mettre sur pied un plan d'action. Nous pourrions, dans six mois ou d'ici un an, juger de la façon dont ce partenariat se sera formé. Ce sera la première indication importante de notre succès.

Q : Quel délai tentez vous de respecter ?

M. HUNKER : Il est court parce que le danger dont s'inquiète le président des attaques électroniques coordonnées, sophistiquées contre les infrastructures de base du pays existe d'ores et déjà. Le président a préconisé un plan national comportant des mesures initiales pour nous protéger, d'ici à l'an 2000, contre les nouveaux types d'attaques cybernétiques. Et il a demandé que, d'ici à 2003, nous disposions de moyens complets de protection de la nation. La menace à laquelle nous devons faire face ne fait que croître avec le temps. Nous devons donc réagir d'urgence et obtenir très rapidement des résultats concrets pour la combattre.

Q : Je crois comprendre que vous comptez avoir quelque chose de prêt en novembre.

M. HUNKER : C'est exact. En fait, l'une des premières choses que le président nous a demandé de faire, en mai, était d'obtenir qu'en l'espace de six mois, soit à la mi novembre, les agences du gouvernement fédéral aient fait d'importants progrès dans l'élaboration de

leurs propres plans pour protéger leurs infrastructures fondamentales. Cela signifie que les ministères de la défense et des finances, entre autres, auront alors mis un dispositif en place pour se protéger d'une attaque électronique. Secundo, le président nous a demandé de poser les bases d'un plan national plus vaste impliquant une collaboration étroite avec le secteur privé, l'intégration du travail d'un certain nombre d'agences et la participation des milieux universitaires, de la recherche et autres ; ce programme comporte donc de nombreux éléments. Notre plan national ne sera pas en place en novembre, mais nous aurons franchi de nombreuses étapes en vue de sa mise au point.

Q : Comment évaluez vous le caractère et la gravité des menaces qui pèsent sur les infrastructures de base des Etats-Unis et quels sont les secteurs les plus vulnérables ?

M. HUNKER : Pour comprendre ces menaces et la vulnérabilité de nos principales infrastructures, nous devons commencer par comprendre la façon dont l'économie a évolué. Depuis deux ans, avec le développement d'Internet, dont l'usage et la taille doublent tous les dix mois, les services fondamentaux dont dépendent les Américains comme l'électricité, notre système bancaire, notre réseau de télécommunications, sont tous liés. C'est sur ces systèmes que reposent notre croissance économique et notre sécurité nationale et ils sont actuellement extrêmement vulnérables.

Nous avons eu un cas, au début de cette année, où durant le renforcement de nos moyens militaires face aux actions de l'Irak, nous nous sommes rendu compte que des pirates s'étaient introduits dans des ordinateurs névralgiques du ministère de la défense. Cette question a occupé pendant plusieurs semaines les plus hauts échelons du ministère de la défense tandis que l'on cherchait à découvrir les sources de ces intrusions. Venaient elles de l'Irak ou de ses alliés ? Il s'avéra que les coupables étaient deux adolescents américains aidés par les conseils d'une personne résidant à l'étranger. Mais cela vous donne une idée du genre de vulnérabilité qui existe.

Dans le Massachusetts, un autre adolescent réussit à paralyser une grande partie du réseau téléphonique de l'Etat et, ce faisant, à interrompre pendant un certain temps le réseau de télécommunications d'un important

aéroport, menaçant ainsi la sécurité des transports aériens. Si des pirates isolés peuvent causer ce genre de tort, songez aux conséquences d'une attaque sophistiquée, organisée, visant à anéantir d'importantes portions de notre réseau électrique ou de télécommunications ou à s'introduire dans des ordinateurs névralgiques. Tel est le genre de menace qui pèse sur nous. Et il existe de nombreux indices du fait qu'il y a, dans d'autres pays, des gens qui sont conscients de cette possibilité de lancer des attaques cybernétiques contre les Etats-Unis et qui s'y préparent.

Q : En tant que directeur du CIAO, vous coordonnez un programme national d'éducation et de prise de conscience du problème. Quel est votre message et comment le communiquez vous au public américain ?

M. HUNKER : Il importe, quand nous parlons d'éducation et de prise de conscience, de faire passer deux messages distincts. L'un est la prise de conscience du problème. Nous vivons dans une nouvelle ère et c'est un type de menace qui n'est devenu que depuis peu un grave sujet de préoccupation. C'est pourquoi la prise de conscience fait partie de notre message. J'ai été très heureux de constater cependant, dans mes conversations aux niveaux supérieurs du gouvernement, que les gens comprennent la nature de cette menace. Et les cadres d'affaires et dirigeants universitaires la comprennent également.

Notre second message est le suivant : Que pouvons nous faire pour déjouer cette menace ? Et c'est la raison pour laquelle nous formons un partenariat entre le secteur privé et les différentes agences gouvernementales afin de prendre des mesures effectives, dans les mois et les années qui viennent.

Q : Dans quelle mesure dépendons nous des ordinateurs, non seulement dans notre vie privée, mais pour le fonctionnement de base de notre société ?

M. HUNKER : Observez ce qui se passe chez vous, dans n'importe quel bureau que vous utilisez. Vous y constatez notre dépendance à l'égard de l'électronique. Nous allons à la banque et utilisons le distributeur automatique de billets ; c'est un système électronique national et international. Notre réseau électrique est de plus en plus géré par Internet. Les transports aériens et ferroviaires dépendent tous de réseaux électroniques. Et

même les entreprises qui n'ont rien à voir avec les ordinateurs ou les logiciels dépendent, pour leur fonctionnement et leur productivité, de systèmes informatiques interconnectés.

On estime qu'entre un tiers et la moitié de la croissance économique que notre pays a connue ces deux dernières années, la création de centaines de milliers d'emplois, sont dus au commerce électronique. C'est la base de notre croissance économique future. C'est aussi la base de notre mission de sécurité nationale, qu'il s'agisse de déplacer du personnel et du matériel à travers le monde ou de rassembler des renseignements essentiels sur les menaces. Tout cela est basé sur ces nouveaux systèmes électroniques.

Q : Comment collaborez vous avec les secteurs commerciaux et industriels pour renforcer la protection des réseaux d'information et de communication des Etats-Unis ?

M. HUNKER : Une collaboration très étroite avec le secteur privé est véritablement au centre des objectifs et de la mission que le président a fixés. Cela peut paraître étrange, mais on peut dire avec exactitude que de 90 à 95 pour cent des systèmes de communication du ministère de la défense appartiennent à des organismes privés et sont gérés par eux. Une telle collaboration est indispensable. Sans le secteur privé, nous n'irions pas très loin.

Je participe actuellement à une série de réunions avec d'autres responsables de divers ministères, notamment les finances et les transports, et avec des cadres du secteur privé, dans des industries telles que les banques et les transports, par exemple, pour créer un partenariat entre le gouvernement et le secteur privé.

En septembre, je me suis rendu à Charlotte (Caroline du Nord) où j'ai rencontré le maire et d'autres personnalités locales, ainsi que les directeurs de plusieurs grosses banques. Charlotte est le deuxième centre bancaire des Etats-Unis. Ma visite avait pour but de m'assurer de la participation des principales banques de Charlotte à ce partenariat.

C'est une tâche de longue haleine. Constituer des partenariats, en particulier dans des domaines dans lesquels nous n'avons pas collaboré préalablement, ne se

fait pas du jour au lendemain. J'ai été très heureux, toutefois, de la réaction que j'ai obtenue, de la prise de conscience et de la coopération des chefs d'entreprise et des cadres de toutes les industries avec lesquelles nous travaillons.

Q : Le CIAO collabore-t-il avec les universités pour aider à trouver des moyens de sécuriser l'information et autres infrastructures clés ?

M. HUNKER : Les milieux universitaires sont un autre élément important du partenariat que nous essayons de former. En fait, en septembre, je me suis entretenu personnellement avec les chanceliers et doyens de plusieurs grandes universités, l'université de Caroline du Nord, l'université Purdue, le Massachusetts Institute of Technology, l'université de Virginie, pour n'en citer que quelques unes. Et cela pour deux raisons. Nous souffrons actuellement, dans ce pays, d'une grave pénurie de spécialistes de l'informatique, des techniques informatiques. Et la menace d'une attaque cybernétique ne va qu'aggraver cette pénurie. Cela va entraîner un accroissement de la demande de personnes ayant la formation nécessaire. Et ce seront principalement les universités qui forment le genre de personnes dont nous allons avoir besoin.

Nous allons également avoir besoin du type de recherche et de développement qui nous permettra de trouver de nouvelles solutions, de mettre au point de nouvelles techniques pour protéger nos systèmes informatiques. Et l'université jouera également un rôle clé dans ce domaine.

Q : En tant que directeur du CIAO, vous avez pour responsabilité d'élaborer des initiatives législatives. Comment collaborez vous avec le Congrès et comment évaluez vous son influence sur la politique et la stratégie liées aux objectifs de CIAO ?

M. HUNKER : La collaboration avec le Congrès est un élément important de ce programme. Et je dois dire que l'intérêt porté à cette question par le Congrès est très élevé et qu'il nous a extrêmement soutenus face à cette nouvelle forme de terrorisme ou de danger pour notre sécurité nationale. Je m'attends à ce qu'il y ait plusieurs domaines importants dans lesquels nous allons travailler avec le Congrès, manifestement sur le plan des ressources.

Dans le cadre du travail que nous accomplissons, nous nous attendons à ce que, dans son budget pour l'exercice 2000, le président inscrive une initiative majeure pour protéger nos infrastructures de base. Cela comprendra des ressources pour la recherche et le développement, pour de nouveaux programmes de formation d'informaticiens, à la fois pour le gouvernement fédéral et pour le secteur privé, peut être d'autres initiatives. Le soutien du Congrès sur le plan des ressources va donc être très important.

Le Congrès va également passer en revue les lois actuelles qui traitent de la sécurité informatique. Un pirate passe souvent par un certain nombre d'ordinateurs avant de parvenir à celui dans lequel il s'introduit. Avec la législation actuellement en vigueur, si nous voulons traquer un pirate, et si ses activités ont eu lieu dans plusieurs Etats, nous devons obtenir des autorisations de perquisition dans chacun de ces Etats pour faire notre travail. Nous allons travailler étroitement avec le Congrès pour examiner toutes les procédures et protections juridiques actuellement en vigueur.

Q : Percevez vous la nécessité d'une plus grande collaboration et coopération internationales dans la protection des infrastructures clés et, dans l'affirmative, comment peut on y parvenir ?

M. HUNKER : L'aspect international du problème est présent dans tout ce qui touche au cyberspace. Nous parlons d'une menace susceptible de venir aussi bien de l'étranger que de l'intérieur du pays, mais qui n'exige pas nécessairement que ses auteurs se trouvent à proximité de l'institution ou de l'infrastructure qu'ils visent.

Nous avons eu, l'année passée, le cas d'un pirate qui se trouvait en Allemagne, mais qui était, en fait, un ressortissant indien, et qui s'était introduit dans un réseau financier de Miami pour tenter d'extorquer des fonds. Dans ce cas particulier, deux pays et les ressortissants de trois pays étaient impliqués dans un incident qui s'attaquait directement à une institution américaine. Cela n'est qu'un petit exemple de l'aspect international du problème.

La Commission présidentielle sur la protection des infrastructures de base a publié son rapport l'an dernier

après avoir étudié ce problème pendant deux ans. Ses recommandations revêtaient une importance clé pour le programme annoncé en mai dernier par le président. Ses auteurs reconnaissent l'extrême importance de la dimension internationale de la question.

Le président a demandé au département d'Etat d'entamer des discussions avec les autres pays au sujet du partage des renseignements et de la possibilité de conclure de nouveaux traités ou protocoles pour répondre aux différents types d'actes de terrorisme ou autres attaques possibles. Un certain nombre de pays nous ont déjà fait part de leur intérêt. Je me suis entretenu personnellement de la question avec des représentants des gouvernements canadien et mexicain et je sais que des discussions ont eu lieu dans le cadre de l'OTAN et d'autres organisations internationales à ce propos.

Cette question suscite donc beaucoup d'intérêt, mais nous n'en sommes qu'aux tout premiers stades de l'élaboration d'un programme international.

Une autre question importante est le chevauchement des efforts que nous faisons pour nous protéger d'une part d'une attaque cybernétique, qu'elle vienne d'une organisation de malfaiteurs, de groupes terroristes ou d'un gouvernement étranger, et d'autre part de ce que l'on appelle le bogue de l'an 2000. Ce cas est très particulier parce que nous savons exactement ce qui va se produire. Et c'est un problème dont nous portons la responsabilité parce qu'il y a des années, les programmeurs n'ont pas tenu compte du fait que l'an 2000 aurait une série de dates différentes de celles de l'an 1900 (un grand nombre de systèmes informatiques anciens ont été programmés pour reconnaître les années par leurs deux derniers chiffres).

Mais, à bien des titres, remédier au bogue exige le même genre de mesures que nous protégeons d'une attaque cybernétique. Les institutions, les entreprises et le gouvernement fédéral doivent commencer à identifier leurs systèmes et la façon dont ils sont interconnectés et décider quels sont ceux d'entre eux qui sont les plus importants à protéger et comment les protéger.

Un autre aspect du problème de l'an 2000 qui se confond avec la menace d'une attaque cybernétique est la création de moyens nationaux permettant de réagir et de rebâtir les systèmes si les réseaux informatiques sont paralysés en l'an 2000. Ce sera le modèle d'une réponse nationale à une attaque cybernétique. Cela mettra en jeu les industries clés, les urgences au niveau des Etats et des municipalités, et les principaux organes du gouvernement fédéral. En fait, mon bureau travaille très étroitement avec John Koskinen, conseiller spécial du président pour les questions liées à l'an 2000, sur divers aspects de ce chevauchement du problème du bogue et des attaques cybernétiques. ●

LE PROBLEME DE L'AN 2000

John Koskinen

Président du Conseil présidentiel sur la transition à l'an 2000

Selon M. Koskinen, l'obstacle principal qui s'oppose à une transition harmonieuse des systèmes informatiques à l'an 2000 est l'ignorance générale de la gravité du problème, qui risque d'entraîner la réalisation des pires scénarios. Pourtant, en agissant dès maintenant, il est encore possible d'en minimiser les effets perturbateurs et d'assurer un passage sans accroc à l'an 2000.

Le monde est confronté aujourd'hui à l'un des grands problèmes de l'âge de l'information. Alors que nous abordons un nouveau millénaire, un nombre incalculable de systèmes informatiques ainsi que les puces codées qui font pratiquement tout marcher, des ordinateurs personnels aux appareils ménagers en passant par les machines industrielles de pointe, sont programmés pour faire marche arrière dans le temps.

Le problème vient du fait que la plupart des vieux systèmes informatiques et microprocesseurs comme on appelle les puces informatiques n'utilisent que les deux derniers chiffres d'une année pour représenter la date. En conséquence, lorsqu'on arrivera à l'an 2000, ces puces pourraient interpréter 00 comme étant 1900 et non 2000. Les défaillances qui en résulteront risquent de perturber gravement les réseaux d'électricité, les usines de traitement des eaux usées, les systèmes financiers, les réseaux de télécommunications et les contrôles de la navigation aérienne dans le monde entier. Chaque pays connaîtra sans doute son lot individuel de mésaventures, mais dans un sens très réel la communauté mondiale tout entière sera affectée.

Comment les programmeurs de logiciels ont-ils pu commettre une erreur aussi évidente? Il y a trente ans, les ordinateurs possédaient beaucoup moins de mémoire qu'ils n'en ont aujourd'hui, si bien que les informaticiens ont recouru à des raccourcis, tel la désignation de l'année par ses deux derniers chiffres, pour économiser de la place. Ils supposaient que les programmes qu'ils concevaient alors seraient de toute façon dépassés et remplacés par de nouveaux logiciels bien avant la fin du siècle. Or, dans la pratique, un grand nombre des grosses installations informatiques complexes, telles que celles utilisées par les banques, les

compagnies d'assurance, ou les sociétés de courtage ont évolué avec le temps, les nouveaux logiciels s'ajoutant aux systèmes existants. Par conséquent, toute organisation dotée de systèmes informatiques de grande échelle et interconnectés devra vérifier des millions de lignes de programmation pour déterminer la façon dont les dates ont été écrites, puis récrire les programmes afin de corriger le problème, ensuite exécuter ces programmes pour voir comment ils fonctionnent, et vérifier l'interface de chaque programme avec les applications internes et externes qu'il utilise.

Sur le plan technique, ces corrections ne sont pas difficiles, mais du fait de l'échelle immense du problème, nous sommes confrontés à un défi colossal sur le plan gestionnel et organisationnel. Pour ne citer qu'un exemple, il n'existe pour réparer le problème qu'un nombre limité de spécialistes qualifiés, de programmeurs connaissant des langages informatiques qui sont peut-être désuets depuis longtemps.

Afin de coordonner les travaux qui s'imposent dans ce domaine au sein de la pléthore de systèmes informatiques que possède le gouvernement fédéral des Etats-Unis, le président Clinton a constitué un conseil regroupant plus de trente organismes. Son premier objectif consiste à assurer le maintien des services publics essentiels, à savoir, veiller à ce que les prestations de maladie et les allocations de chômage continuent d'être versées et que la collecte des impôts ne subisse aucune interruption. Le président a fixé l'objectif ambitieux de faire en sorte que la totalité des systèmes informatiques fédéraux soient « conformes à l'an 2000 », c'est à dire réparés, avant la fin de mars 1999. Le conseil s'est également divisé en groupes de

travail chargés de se concerter avec les autorités locales sur ce problème et d'évaluer les efforts que déploient les entreprises privés dans trente cinq secteurs d'industrie, tels que les transports, les télécommunications et les finances.

En outre, l'état d'avancement des travaux sur ce problème à l'étranger nous intéresse beaucoup, puisqu'une multitude de systèmes informatiques ont aboli les frontières, si bien qu'aucun pays n'échappe à cette interdépendance. Nous avons pressenti les organisations internationales afin de faire face à ce problème. Les Nations unies ont adopté une résolution invitant tous les Etats membres à prendre des mesures et à rendre compte de leurs résultats à l'Assemblée générale avant le 1er octobre. Afin de sensibiliser les Etats à ce problème, la Banque mondiale met sur pied une vingtaine de conférences régionales à l'organisation desquelles les Etats-Unis apportent leur appui sous la forme d'une contribution de douze millions de dollars. Le Fonds monétaire international a décidé de ne ménager aucun effort en vue d'encourager les pays à consacrer des ressources à ce dossier. La secrétaire d'Etat, Mme Madeleine Albright, a envoyé à toutes les ambassades des Etats-Unis de par le monde des instructions aux ambassadeurs leur demandant de s'enquérir du degré de préparation de chaque pays. L'Agence d'information des Etats-Unis dirige au sein du conseil présidentiel un groupe de travail chargé de la communication, de la diffusion d'informations et de l'aide à la conception de plans d'urgence en collaboration avec les autres pays.

Malheureusement, à ce stade, il reste moins de cinquante jours avant le 1er janvier 2000. Je constate que, dans nombre de pays, l'obstacle majeur se situe encore au niveau de la prise de conscience des autorités publiques, des journalistes, des industriels et du grand public. La première étape, pour les Etats comme pour les entreprises privées, doit être de faire l'inventaire de toutes leurs opérations faisant appel à l'informatique et d'élaborer un programme de réparation. Une deuxième étape vitale concerne l'élaboration de plans d'urgence. Le conseil présidentiel a demandé à chaque organe du gouvernement fédéral de concevoir deux plans. Le premier est interne: que faire si certains de nos systèmes informatiques ne fonctionnent plus? Le second est externe: que faire en cas de défaillance de systèmes informatiques extérieurs liés aux nôtres?

On peut s'attendre que les perturbations liées à l'an 2000 débiteront avant le nouveau millénaire, lorsque des systèmes informatiques désuets essaieront de faire des calculs prévisionnels ou de prévoir des événements futurs. On relève aux Etats-Unis un certain nombre de sites d'Internet où des spécialistes que l'on ne saurait normalement qualifier d'alarmistes annoncent des défaillances généralisées de systèmes informatiques provoquant des pannes d'électricité, des embouteillages, une récession économique, voire, dans certaines régions, des pénuries alimentaires. Personnellement, sans rejoindre les rangs des oiseaux de mauvais augure, je m'inquiète surtout des pays où l'inaction et l'absence de prise de conscience risqueraient de précipiter la réalisation de ces scénarios funestes. En prenant des mesures dès aujourd'hui, nous arriverons à éviter le chaos et, avec un peu de chance, à effectuer une transition sans accroc à l'an 2000. ©

LA MENACE DE CYBERGUERRE APPELLE TOUS LES SECTEURS A UNE VIGILANCE CONSTANTE

Entretien avec le sénateur Jon Kyl

Ni le gouvernement américain, ni le Congrès, ni le grand public ne prêtent suffisamment d'attention à la menace croissante de cyberguerre, affirme le sénateur Jon Kyl. Selon lui, en effet, des adversaires en puissance perfectionnent actuellement les moyens de s'attaquer à l'infrastructure de base qui gère les réseaux de communication, des transports et des banques ainsi que la défense nationale des Etats-Unis. Le sénateur républicain de l'Arizona préside la sous-commission sur la technologie, le terrorisme et l'information au sein de la commission judiciaire du Sénat. Il siège également à la commission sénatoriale du renseignement. M. Kyl a répondu aux questions que lui posait Ralph Dannheisser, collaborateur de la rédaction.

QUESTION : En juin dernier, lors d'une séance de la commission, vous avez déclaré que le système informatique des Etats-Unis était plus vulnérable à une attaque que leur appareil militaire. Pourriez-vous entrer dans les détails à ce sujet ?

M. KYL : Cette opinion est largement partagée. Nous avons la puissance militaire la plus forte du monde et personne ne serait capable de nous attaquer sur ce plan. La question est donc la suivante : Un adversaire éventuel chercherait-il à atteindre les points les plus vulnérables des Etats-Unis s'il voulait nous attaquer ? Cette question vaut également pour les terroristes. La réponse est que notre infrastructure informatique est l'un de nos points vulnérables parce que nous dépendons plus qu'aucun autre pays de la technologie de pointe pour nos communications, nos transports, nos transactions financières, y compris, bien sûr, notre défense. La vulnérabilité de notre infrastructure informatique est donc probablement l'une des principales cibles que choisirait un pays agresseur ou une organisation terroriste.

QUESTION : Dans la même veine, vous avez déclaré qu'il s'agissait du problème de sécurité nationale et de sécurité publique le plus grave auquel notre pays aurait à faire face dans les années qui viennent. Que redoutez-vous le plus si on ne s'attaque pas comme il convient à ce problème ?

M. KYL : Commençons par le passage au XXI^e siècle. Le bogie de l'an 2000, que l'on a identifié à juste titre comme un sérieux problème en puissance pour notre

pays, est aggravé par le fait qu'il donnera aux terroristes et autres groupes de gens ou individus qui nous veulent du mal une occasion merveilleuse de lancer une attaque à un moment où notre pays sera plongé dans une confusion maximum. Nous ne saurons pas à quoi attribuer tout ce qui se détraquera à minuit, le 31 décembre 1999. Nous attribuerons probablement la plupart des problèmes au bogue, mais cela fournira manifestement à ceux qui nous veulent du mal une bonne occasion de sabotage ou d'attaque de notre infrastructure, à la fois parce que leurs activités seront couvertes par cet événement et en raison de la position vulnérable dans laquelle nous mettra l'événement lui-même.

C'est donc la première grande possibilité qui se présentera. Mais en dehors de ce moment là, du fait que, comme je l'ai dit à propos de la vulnérabilité des différents aspects de notre société civile et de certains éléments de notre défense, s'attaquer à notre infrastructure est l'un des meilleurs moyens de nous nuire dans l'abstrait, si un conflit était en cours, cela offrirait à nos adversaires une merveilleuse occasion de nuire à notre capacité de faire face aux menaces en jeu.

Q : Est-il facile, dans l'ensemble, de faire intrusion dans le réseau informatique à un moment quelconque et quel genre de dommages celui qui y parviendrait pourrait-il causer ?

M. KYL : Chose étonnante, c'est très facile. Il est difficile de quantifier ces dommages, mais on a récemment procédé à des exercices dans ce domaine. L'un de ces

exercices, qui a eu lieu dans les médias, a prouvé, en termes très réels, à quel point les réseaux de transports, d'électricité et autres sont vulnérables à une attaque émanant de pirates, en d'autres termes de gens qui utilisent un équipement courant, et non du matériel d'espionnage. L'équipement actuellement disponible peut permettre de perturber des aspects essentiels de notre infrastructure informatique. Dans le cadre de l'exercice en question, une partie du réseau d'électricité, du réseau de transports et du réseau financier a été perturbée. D'autres domaines vulnérables sont les systèmes d'approvisionnement en eau, toutes les formes de télécommunications, bien sûr, ainsi que les urgences, mais du point de vue de la défense, rien n'est plus grave sans doute que la menace qui pèse sur nos laboratoires militaires et nos systèmes d'armes.

Il existe donc un degré élevé de vulnérabilité et chaque fois qu'un jeune pirate étranger s'introduit dans le système informatique du Pentagone, les gens se grattent la tête et se demandent comment cela peut se produire. Ils tirent ensuite des leçons de cette expérience, mais cela semble être un apprentissage constant. Je vous donne une autre illustration du problème : juste avant les préparatifs de février dernier concernant l'Irak, alors que nous nous préparions à intervenir contre Saddam Hussein, une intrusion dans les ordinateurs du Pentagone a été si grave qu'on a prévenu le président qu'il pouvait s'agir d'un acte délibéré du gouvernement irakien. Pendant un certain temps, nous nous sommes demandé si l'Irak était à l'origine de cet incident. Il s'avéra que c'était l'œuvre de trois jeunes gens de trois pays différents. Vous m'avez demandé à quel point nous étions vulnérables. Je pense que cela répond à votre question.

Q : Il est certain que si des jeunes n'ayant aucun mobile funeste peuvent pénétrer si facilement dans le système informatique du Pentagone, cela montre que nos adversaires pourraient le faire tout aussi aisément avec des conséquences beaucoup plus graves.

M. KYL : C'est précisément ce qu'on craint.

Q : Du fait de votre poste de président de la commission et étant donné le grand intérêt que vous portez à la question, pouvez-vous nous dire quel rôle le Congrès devrait jouer, selon vous, pour nous protéger contre ce genre de guerre cybernétique ou de cyberterrorisme ?

M. KYL : Il est évident que nous devons donner aux agences de sécurité nationale, à la défense, les fonds et le pouvoir nécessaire pour faire face à ce problème.

Cela pose quelques problèmes, mais je crois que cela consiste principalement à élaborer la politique gouvernementale, à prendre la question au sérieux et à donner au gouvernement les moyens de l'appliquer.

Nous faisons pression depuis quatre ans sur le gouvernement Clinton et il est encore à la traîne. Il était censé présenter un plan, ce qu'il n'a pas encore fait. Le président avait ordonné qu'un plan soit élaboré dans les 180 jours. C'est ce que nous attendons. Normalement, c'est le 22 novembre que ce plan doit être prêt. Je suppose donc que c'est ce que font actuellement les agences gouvernementales pour régler ce problème entre elles.

Q : Était-ce à l'instigation du Congrès ?

M. KYL : C'est le Congrès qui a fait démarrer l'affaire en demandant à deux reprises au président de lui soumettre un plan ou un rapport sur la question, ce qu'il n'a pas fait. Au lieu de cela, il a nommé une commission et formé un groupe de travail au sein du gouvernement. Parmi leurs recommandations figurait la préparation de ce plan. Ils ont donc projeté pendant longtemps d'entamer ce rapport et nous arrivons à la fin de la période de 180 jours. J'espère que ce plan fournira au moins des directives à toutes les principales agences du gouvernement pour qu'elles traitent avec le secteur privé avec lequel elles ont des rapports et qu'elles lui fournissent des conseils, au moins durant la première phase de cette activité. Mais la défense est toujours absente de ce projet, et c'est sur cela que le gouvernement devra ensuite se concentrer, à mon avis. Notre rôle consiste donc à continuer à exercer des pressions sur le gouvernement et à lui fournir les ressources qui s'avéreront nécessaires.

Q : Pensez-vous que cette question reçoive du Congrès toute l'attention qu'elle mérite ?

M. KYL : Non, mais il ne règne aucun désaccord à ce sujet au sein de la législature. Il s'agit d'un effort commun des deux partis, des deux chambres. Il n'y a donc là aucun problème. Mais si vous me demandez si l'on comprend suffisamment ce problème au Congrès ou

dans le public en général, je vous répondrai par la négative. Et il existe également une insuffisance de compréhension ou d'engagement de la part du gouvernement.

Q : Vous y avez fait allusion, mais étant donné l'interconnexion de l'infrastructure informatique, les secteurs public et privé doivent-ils coordonner leurs activités dans ce domaine et travailler de concert ?

M. KYL : Oui, c'est nécessaire. Et nous espérons qu'une partie du plan du gouvernement traitera de cet élément de coordination. On peut supposer, par exemple, que le ministère des transports aura un plan qui intégrera les composants de l'industrie des transports avec ses propres activités pour assurer une action commune. Il y a également un groupe industriel qui intervient principalement dans le domaine des télécommunications et qui a depuis longtemps des rapports à ce sujet avec le président. Ce groupe continue à donner de nombreux conseils sur ce dont le secteur privé a besoin et sur ce qu'il peut faire dans ce domaine. Parce qu'en définitive, c'est l'équipement, la technologie produite par le secteur privé qui sont utilisés à la fois par le secteur public et le secteur privé et ce dernier peut faire preuve de beaucoup d'innovation dans ce qu'il incorpore dans ses systèmes et dans les solutions qu'il propose au gouvernement. C'est ce qui se passe actuellement.

Q : Vous avez mentionné précédemment un soupçon, qui s'est avéré sans fondement, et selon lequel l'Irak se serait livré à certaines activités dans le domaine de la cyberguerre. Y a-t-il, à votre connaissance, des adversaires des Etats-Unis qui procèdent activement à ce genre de préparatifs à l'heure actuelle, et quelle serait la nature de ces activités ?

M. KYL : Selon nos services de renseignement, de nombreux pays s'intéressent aux techniques de la cyberguerre et il y a un nombre moins important de pays qui visent explicitement les Etats-Unis dans leur planification. Je ne saurais dire si un pays quelconque a tenté d'attaquer notre infrastructure informatique.

Q : Je suppose que les attaques consisteraient soit à détruire certains domaines d'activité qui sont contrôlés par le système informatique soit à y introduire des données fausses.

M. KYL : Les agresseurs pourraient pénétrer dans le système et obtenir des informations, y introduire soit toutes sortes de virus qui entraveraient ou paralyseraient les opérations, soit des informations fausses. Ils pourraient donc faire ces trois choses.

Q : Et je présume qu'il y a, quelque part, quelqu'un qui étudie ce genre d'activité.

M. KYL : Comme je l'ai dit, un grand nombre de pays ont des programmes de ce genre en cours, dont certains visent les Etats-Unis. Cela ne veut pas dire que ces pays tentent aujourd'hui d'attaquer les Etats-Unis. Je dis simplement qu'ils ont mis au point des programmes, ou sont en train d'étudier le concept d'une cyberguerre contre les Etats-Unis. Il va de soi, et ce sera peut être votre prochaine question, que les Etats-Unis se penchent sur la question en termes offensifs aussi bien que défensifs.

Q : Pourriez-vous développer ce point ?

M. KYL : Je me bornerai à rappeler aux lecteurs qu'évidemment, en ce qui concerne la capacité de mener une offensive cybernétique, nous sommes, et de loin, le pays le plus vulnérable, du fait de notre degré de dépendance par rapport à la technique, si bien que, pour nous, il s'agit plus d'une attitude défensive qu'offensive.

Q : Mais vous laissez entendre qu'on procède cependant à certains préparatifs, à certaines études.

M. KYL : Souvenez vous que, peu après l'opération « Tempête du désert », on a obtenu certaines informations sur le degré de perturbation causé par les Etats-Unis aux communications irakiennes et sur d'autres activités susceptibles d'être considérées, je le suppose, comme le premier exemple du recours à la cyberguerre. Mais ce genre d'activité n'a rien de nouveau. Je veux dire que depuis des années, des décennies même, nous tentons de brouiller les communications de l'ennemi, de percer ses codes, etc. C'est donc la même chose. Il s'agit simplement d'une version beaucoup plus complexe de ce type d'activité.

Q : Que projetez vous comme activités nouvelles, à ce stade, dans votre commission ?

M. KYL :La prochaine chose que nous ferons consistera à étudier le rapport qui sera publié en novembre en réponse à la directive présidentielle et qui nous donnera des indications sur ce que le gouvernement projette de faire, à l'évaluer, peut être à tenir une audition pour nous renseigner sur ses intentions et entendre les exposés de personnes qui pourraient avoir d'autres idées sur la question. Je ne suis pas sûr, pour l'instant, de ce que nous ferons par la suite.

Q : Estimez-vous que d'importantes sommes supplémentaires seront nécessaires à un moment quelconque?

M. KYL :Il s'agira de sommes relativement peu importantes, en fait, mais je pense qu'on aura effectivement besoin de fonds.



DES FANTOMES DANS LES ORDINATEURS ?

Martin Libicki

Directeur du bureau d'analyses à la société RAND

L'auteur considère l'application des lois comme le domaine principal dans lequel la sécurité informatique mondiale peut être renforcée. Il préconise l'harmonisation des lois nationales contre les cyberattaques, la coopération multinationale pour dépister ces attaques à travers les frontières, la conclusion de traités internationaux sur l'extradition des auteurs de telles attaques et l'imposition de sanctions à ceux qui protègent ces derniers. Selon lui, la volonté de partager des renseignements sur la recherche et le développement, les signes avant-coureurs d'attaques et les attaques elles-mêmes ainsi que la réaction qu'elles suscitent peuvent également améliorer l'efficacité des mesures de protection de chaque pays.

Quiconque est à la recherche d'une nouvelle raison de s'inquiéter n'a pas besoin d'aller très loin. Partout, les ordinateurs et autres appareils numériques se sont immiscés dans notre existence. Ce qui était autrefois manuel est maintenant automatique. Ce qui était analogue est à présent numérique ; ce qui était isolé est désormais relié à tout le reste. Il s'avère de plus en plus que nous n'avons d'autre option que de faire confiance à l'informatique. Si elle nous faisait défaut, nous serions perdus.

La foi qu'inspire la dépendance serait méritée si ces appareils ne faisaient que ce qu'ils sont censés faire. Certains tombent en panne d'eux mêmes et nous y remédions. Mais il est également possible qu'ils nous fassent défaut parce qu'ils sont tombés aux mains d'individus aux intentions malveillantes. Dans de telles circonstances, ils risquent non seulement de cesser de fonctionner, mais aussi de révéler des secrets que nous leur avons confiés ou de produire une information corrompue, ce dont on s'aperçoit parfois trop tard pour annuler les mesures qu'il ont déclenchées.

Comment s'explique cette vulnérabilité ? Les ordinateurs sont rapides, peu coûteux, efficaces et ils oublient rarement ce qu'on leur dit. Mais ils sont aussi terriblement littéraux et manquent généralement du discernement nécessaire pour comprendre les conséquences de ce qu'on leur demande de faire ou l'honnêteté de ceux qui leur donnent de tels ordres.

Les conséquences éventuelles de pannes ou de corruption délibérées des systèmes sont vastes. En prenant les commandes des réseaux de base sur lesquels

repose la société, les gens qui s'attaquent aux ordinateurs peuvent, en théorie, écouter les conversations téléphoniques, dérouter les connexions et complètement paralyser les liaisons téléphoniques ; provoquer une panne d'électricité ; bloquer des mouvements de fonds portant sur les billions de dollars qui changent de main chaque semaine ; entraver les services d'urgence ; empêcher l'armée américaine de réagir rapidement à des crises à l'étranger ; révéler des secrets médicaux personnels ; perturber les réseaux de transport et mettre les voyageurs en danger ; et bien d'autres choses encore. La vie telle que nous la connaissons pourrait s'arrêter.

Les attaques cybernétiques, si elles étaient suffisamment systématiques, pourraient être une forme de guerre, d'où la guerre de l'information électronique en tant que concept. Mais prise dans son sens le plus large, la guerre de l'information, c'est à dire une attaque dirigée contre les processus d'information et de décision d'un pays, est aussi vieille que la guerre elle-même. De telles tactiques comprennent les opérations psychologiques, les attaques contre l'appareil de commandement de l'ennemi, l'espionnage et le contre espionnage, et les opérations contre les infrastructures et réseaux de surveillance de l'adversaire. Aux Etats-Unis, durant la guerre de sécession (1861-1865), il y a eu des activités de propagande, des tireurs embarqués à bord de montgolfières visant des généraux et des observateurs, des maraudeurs arrachant les lignes télégraphiques, des détachements et contre attaques de cavalerie, c'est à dire des activités entrant toutes dans le cadre de la guerre de l'information. La Seconde Guerre mondiale a vu l'apparition de la guerre électronique sous forme de

radar, de supercherie électronique, de brouillage des fréquences radio, et même de codage et de décodage assistés par ordinateur.

Les attaques cybernétiques cadrent parfaitement avec ce concept. Si on peut détruire le quartier général de l'ennemi à coups de canon, qu'y a-t-il de répréhensible à utiliser des moyens moins violents pour pénétrer et détruire les systèmes informatiques qui géreront les batailles de demain? A partir de 1920, les stratèges ont prétendu qu'en utilisant la puissance aérienne contre des cibles civiles, on éviterait la boucherie de la guerre de tranchées. La guerre de l'information électronique fait encore mieux.

Les sociétés modernes sont-elles vulnérables? La plupart des systèmes d'information sont beaucoup moins sûrs qu'ils ne pourraient ou ne devraient l'être. Des réseaux et systèmes de nombreux types ont été attaqués: Internet, le service téléphonique, certains services de transport, des institutions financières et des réseaux d'entreprises.

Les attaques cybernétiques sont, à tous points de vue, un grave problème. En fait, le Bureau fédéral d'enquête (FBI) des Etats-Unis a récemment estimé qu'elles coûtaient à l'économie américaine de un demi milliard à cinq milliards de dollars par an, la marge d'erreur de ce chiffre étant importante et très révélatrice. En effet, personne ne sait exactement combien d'attaques se produisent. La plupart des preuves sont anecdotiques et il faut donc extrapoler en recourant à des préceptes populaires tels que «seuls les amateurs laissent des empreintes, pas les professionnels» ou encore: «les gens ne veulent jamais parler de tous les torts qui leur ont été causés». C'est pourquoi les attaques cybernétiques sont comparées à des icebergs, les Etats-Unis étant censés jouer le rôle du Titanic.

C'est du moins la théorie. Mais que nous réserve l'avenir? Contrairement à ce qui se passe dans presque toutes les autres formes de guerre, il n'y a pas d'infraction dans le cyberspace. Si les pirates de l'informatique (les «hackers») s'introduisent dans un système, ils le font en suivant des voies déjà tracées dans ce système; certaines sont des caractéristiques et d'autres des défauts (c'est à dire des caractéristiques non documentées) jamais supprimés. Quoi qu'il en soit, la navigation le long de ces voies est sous le contrôle complet de la personne qui

gère le système. Ceci étant, la vigilance suffit pour assurer sa protection.

En fait, les moyens de protection existent. Un grand nombre de systèmes informatiques opèrent à plusieurs niveaux. Il existe des moyens de dépister les utilisateurs illégitimes, des verrouillages pour empêcher les usagers légitimes de prendre délibérément ou par inadvertance le contrôle de systèmes informatiques, ainsi que des dispositifs de sécurité qui permettent d'éviter que l'usurpation du contrôle ne crée un danger public.

Les pirates, pour leur part, doivent d'abord tromper un système en se faisant passer pour des usagers légitimes (en volant ou en devinant un mot de passe, par exemple), puis acquérir des privilèges de contrôle (souvent en exploitant des défauts endémiques) refusés à la plupart des usagers courants. Grâce à de tels privilèges exceptionnels, ils peuvent éliminer des fichiers clés, y insérer des inepties, ou encore se ménager une petite porte qui leur permettra de pénétrer de nouveau dans le système.

Il ne fait aucune doute que les défenses dont on peut avoir besoin pourraient être meilleures qu'elles ne le sont en général à l'heure actuelle.

La plupart des systèmes utilisent des mots de passe pour limiter l'entrée, mais ces mots de passe ont de nombreux problèmes bien connus: trop d'entre eux sont facilement devinables, ils peuvent être volés s'ils circulent sur le réseau, et sont trop souvent conservés dans des endroits prévisibles sur un serveur. Les méthodes cryptographiques telles que les signatures numériques permettent d'éviter ces problèmes (l'astuce consistant à capter et réutiliser les messages d'accès ne marche pas.) Les signatures numériques aident même à assurer que tout changement apporté à une base de données ou à un programme, une fois signé électroniquement, permet de remonter à son auteur, ce qui est également utile si le pirate est dans la place, s'il s'agit de quelqu'un à qui on a accordé des privilèges d'accès au système.

Les systèmes d'ordinateurs et d'exploitation de réseaux sont vulnérables à l'insertion par les pirates de programmes comme les virus (logiciels qui infectent les programmes qui, à leur tour, en contaminent d'autres) les chevaux de Troie (logiciels en apparence utiles, mais contenant des pièges cachés), et des bombes logiques

(logiciels qui restent en sommeil jusqu'à ce qu'on les active). Les programmes de protection contre les virus peuvent être efficaces, mais si on craint ces derniers, pourquoi ne pas conserver tous les fichiers importants sur un dispositif inaltérable (par exemple un CD ROM)? Un tel dispositif peut aussi empêcher l'effacement ou la corruption de l'information par les empreintes numériques d'un pirate en puissance. En fait, étant donné le faible coût de tels dispositifs, la perte de l'information n'a plus d'excuse légitime.

Les systèmes peuvent aussi être menacés par d'autres systèmes considérés comme fiables. Deux précautions peuvent être prises contre ce danger : sélectionner les systèmes dignes de foi et limiter le nombre de messages auxquels un système réagira. C'est ce que font les banques, par exemple, pour empêcher la corruption de leurs ordinateurs par les distributeurs automatiques de billets. L'ordinateur ne tient compte d'aucun message d'un distributeur qui ne serait pas une transaction légitime. Aucune transaction légitime ne peut corrompre l'ordinateur de la banque.

Une précaution finale consiste à débrancher les ordinateurs du réseau. En dernier ressort, un grand nombre de systèmes informatiques (comme ceux des centrales nucléaires) fonctionnent presque aussi bien s'ils ne sont pas reliés au monde extérieur.

Jusqu'où les propriétaires d'un système doivent-ils aller? Des mesures de sécurité peu coûteuses (filtres sécuritaires et détecteurs d'intrusion) peuvent paraître suffisantes pour l'environnement courant. Après tout, dépenser des sommes énormes pour protéger un système est injustifié si une attaque ne ferait que perturber temporairement le service. Un grand nombre d'entreprises ne s'attendent à aucune menace grave et investissent en conséquence. Elles ont peut-être raison. Mais si elles avaient tort? Si les menaces s'accroissent, les propriétaires de systèmes peuvent accroître la sécurité, même à court terme (par exemple en empêchant les utilisateurs d'entrer dans le système à partir de chez eux ou de procéder à certaines manœuvres une fois entrés).

En fait, c'est précisément l'absence de bons éléments de sécurité dans l'infrastructure nationale de l'information qui incite à penser que les systèmes pourraient, en cas de besoin, être sécurisés davantage. (En revanche, les

moyens efficaces de défense contre la guerre nucléaire ont été techniquement inexistantes pendant des décennies et, s'ils existent aujourd'hui, ils sont néanmoins très coûteux.) Même si le fonctionnement de nombreux systèmes peut être temporairement paralysé, faire durer la panne tandis que ses gestionnaires s'emploient fiévreusement à rétablir les services essentiels est une autre histoire. Quiconque pense que l'infrastructure informatique des Etats-Unis est en péril doit savoir que la simple menace d'une attaque, si elle est prise au sérieux, s'estompe peu après avoir été proférée, aussitôt qu'on y réagit.

Quel devrait être le rôle du gouvernement? Les services responsables de la protection du pays au sol, sur mer, dans les airs et dans l'espace extra atmosphérique peuvent-ils aussi protéger le pays dans le cyberspace? Devraient-ils le faire?

Le gouvernement peut être utile dans ce domaine, mais il y a beaucoup de choses qu'il ne peut ou ne devrait pas faire. Certes, l'électricité est indispensable, mais mettre son approvisionnement à l'abri des pirates dépend presque entièrement de la façon dont les compagnies d'électricité gèrent leurs systèmes informatiques. Ceci comprend le réseau et les logiciels qu'elles acquièrent, la configuration de ces logiciels, la façon dont les privilèges d'accès au réseau sont accordés et protégés et dont les divers mécanismes à sûreté intégrée et manuels sont disséminés à travers le réseau de production et de distribution des compagnies. Il est inconcevable qu'une compagnie d'électricité quelconque puisse souhaiter que le gouvernement la protège en lui disant comment procéder. Sur un plan plus général, le gouvernement ne peut entourer les Etats-Unis d'un coupe-feu, ne serait-ce qu'en raison de la multiplicité des réseaux internes qui sillonnent le globe.

Le gouvernement peut réprimer les attaques cybernétiques, ce qu'il fait d'ailleurs, et il a remporté d'importants succès dans ce domaine compte tenu de l'anonymat et de l'éloignement de leurs auteurs. Jusqu'à maintenant, la plupart des attaques qui ont été détectées et ont défrayé la chronique ont été le fait d'amateurs et non de professionnels.

Le gouvernement devrait-il tenter d'enrayer la guerre de l'information électronique en menaçant ses auteurs de représailles, à supposer que l'identité des agresseurs

puisse être établie? Le gouvernement américain peut menacer l'agresseur de lui rendre la pareille, mais un grand nombre d'Etats hors la loi n'ont guère de systèmes comparables susceptibles d'être anéantis (La Corée du Nord, par exemple, n'a pas de marché financier). De même, il serait problématique de répondre violemment à une attaque cybernétique qui aurait fait perdre du temps et de l'argent à sa victime, mais n'aurait blessé personne.

Bien que la plupart des mesures que le gouvernement peut prendre pour accroître la sécurité informatique soient indirectes, la Commission présidentielle pour la protection de l'infrastructure de base et d'autres organismes ont fait les recommandations suivantes :

- s'assurer que les systèmes informatiques du gouvernement soient protégés parce qu'ils sont importants pour la sécurité nationale et pour l'établissement de normes en général,
- utiliser la recherche, le développement et l'acquisition des systèmes par leurs premiers usagers pour promouvoir la mise au point rapide de dispositifs de sécurité,
- diffuser des avertissements en cas d'attaque imminente (à condition qu'une telle menace puisse être détectée ce qui n'est pas facile),
- promouvoir un cadre juridique qui encourage le secteur privé à partager son expérience et ses contre-mesures sur une base confidentielle.

L'adoption de telles mesures progresse, dans l'ensemble.

Malheureusement les restrictions gouvernementales existantes et celles que le gouvernement menace de prendre sur le cryptage à décision formelle ont entravé l'un des meilleurs outils qui existent pour la protection des systèmes et entamé la crédibilité de l'action gouvernementale dans le domaine de les pirates de l'informatique.

Activités internationales : Etendre la plupart de ces mesures gouvernementales à l'étranger implique l'élaboration d'un programme pour guider la lutte internationale contre la guerre de l'information.

L'application des lois est un vaste domaine.

L'harmonisation des lois nationales contre les attaques cybernétiques, la coopération nationale visant à entraver les attaques en provenance de l'étranger, les traités internationaux sur l'extradition des pirates et la volonté d'infliger des sanctions à ceux qui protègent ces derniers peuvent toutes accroître la sécurité mondiale de l'information.

La volonté de partager les informations sur la recherche et le développement, sur les signes avant-coureurs d'attaques, les avertissements et les attaques elles-mêmes ainsi que les réactions qu'elles suscitent peuvent également accroître l'efficacité des mesures de protection de tous les pays. Cependant ces domaines sont souvent du ressort des agences de renseignement, qui ne sont guère connues pour leur transparence.

Conclusions et pronostics : Dans le monde de l'après-guerre froide, on assiste à un accroissement de menaces nouvelles et peu conventionnelles (par exemple des terroristes équipés d'armes nucléaires) qui sont inquiétantes, mais jusqu'à présent théoriques. La guerre de l'information en fait partie. Plus les systèmes d'information envahissent la société sa défense, son commerce, sa vie au quotidien et plus leur sauvegarde revêt d'importance. L'éventualité d'actes de malveillance extrême existe, particulièrement quand ils risquent d'être perpétrés systématiquement par un adversaire disposant de gros moyens financiers. Mais ce qui frappe aussi, c'est le fait que bien que la guerre de l'information soit relativement peu coûteuse, les incidents réellement préjudiciables ont été rares, jusqu'à maintenant.

Deux indices peuvent nous renseigner à fond sur la probabilité d'une attaque cybernétique. L'un d'eux est la façon dont les gens réagiront au bogue de l'an 2000. Supposons qu'une grande partie des systèmes informatiques du monde s'effondrent à minuit, le 31 décembre 1999. La panique et la paralysie en résulteront-ils ou les gens trouveront-ils rapidement des moyens de contourner le problème ou de se passer pendant un certain temps de l'informatique? Si les procès se multiplient, quels précédents va-t-on établir pour attribuer la responsabilité des torts causés par l'effondrement du système?

L'autre pronostic est d'origine plus récente. L'auteur le

plus plausible de graves actes de terrorisme cybernétique serait quelqu'un qui n'aurait rien à perdre (c'est à dire pas un pays), posséderait plusieurs centaines de millions de dollars de fonds cachés, des connaissances techniques, un réseau d'amis malhonnêtes et qui aurait un compte (réel ou

imaginaire) à régler avec les Etats-Unis ou un autre pays. Cela vous paraît il familier? Dans l'affirmative, ce qui se passera l'année prochaine montrera peut être si des individus ou groupes puissants pourront tenter de ruiner un pays en recourant à la guerre de l'information ou s'ils dirigeront leurs efforts ailleurs. ●

LA REPONSE DE L'ENSEIGNEMENT SUPERIEUR A LA GUERRE INFORMATIQUE

*Charles Reynolds
Directeur du département d'informatique
et doyen intérimaire de la Faculté des sciences et technologies
intégrées de l'université James Madison*

Il existe une demande croissante de spécialistes en sécurité informatique à une époque où « un vandalisme malveillant, des activités criminelles et une guerre informatique internationale » peuvent tous menacer l'infrastructure informatique de notre pays, affirme M. Reynolds. Il décrit comment le monde de l'enseignement supérieur collabore avec le secteur public comme avec le secteur privé pour répondre à ce besoin au moyen d'une initiative lancée en 1997 et appelée « National Colloquium for Information Systems Security Education », Colloque national pour l'éducation en matière de sécurité des systèmes informatiques, ou NCISSE. L'auteur, qui est président pour 1998 du comité directeur du NCISSE, souligne également les efforts de l'université James Madison, qui s'alignent dans les nouvelles priorités nationales visant à faire face aux menaces contre les réseaux informatiques des Etats-Unis.

LE BESOIN DE PROTECTION DE L'INFRASTRUCTURE DE L'INFORMATION ET DES COMMUNICATIONS

Tous les aspects de nos vies et tous les aspects de nos systèmes sociaux, économiques et politiques dépendent de plus en plus de notre infrastructure d'information et de communications. Nos systèmes financiers, nos systèmes de transport, nos services publics de distribution d'eau et d'électricité, ainsi que toutes les autres infrastructures cruciales dépendent maintenant de notre infrastructure d'information et de communications. Cependant, cette infrastructure est la plus vulnérable de toutes nos infrastructures aux actes de vandalisme malveillant, aux activités criminelles et à la guerre de l'information à l'échelle internationale qui peuvent tous la menacer et qui menacent par conséquent aussi toutes les autres infrastructures qui en dépendent. La sécurité et l'intégrité de notre infrastructure d'information et de communications constituent donc une priorité nationale.

Pour confronter les menaces de cette nouvelle ère de la technologie de l'information, notre pays a besoin d'une main d'œuvre compétente en informatique qui soit au courant des nouvelles vulnérabilités des infrastructures d'importance cruciale, ainsi que de spécialistes de la sécurité de l'information connaissant les « meilleures pratiques » reconnues et disponibles dans les domaines

de la sécurité de l'information et de l'assurance de l'information.

UN DIALOGUE NATIONAL AVEC L'ENSEIGNEMENT SUPERIEUR

En réponse au besoin de protéger les infrastructures d'importance cruciale du pays, le « National Colloquium for Information Systems Security Education » (Colloque national pour l'éducation en matière de sécurité des systèmes informatiques, ou NCISSE) fut créé en mai 1997 pour constituer un forum permettant un dialogue entre des responsables de haut niveau du secteur public, du secteur privé et des universités afin de trouver des moyens de coopérer de manière à définir les besoins actuels et futurs en matière d'enseignement de la sécurité de l'information. Le NCISSE tente également d'influencer et d'encourager le développement et l'expansion de programmes universitaires de sécurité de l'information, tout particulièrement aux niveaux de la maîtrise et du troisième cycle.

Lors de sa deuxième réunion annuelle tenue en juin 1998 à l'université James Madison, située à Harrisonburg, en Virginie, les membres du Colloque se sont mis d'accord pour décider que leur association s'efforcerait d'encourager la création de programmes universitaires reconnaissant les besoins exprimés par le

secteur public et par le secteur privé, sur la base des « meilleures pratiques » reconnues et disponibles en l'état actuel des choses.

Le Colloque fait également porter ses efforts sur la nécessité d'aider les établissements d'enseignement en favorisant le développement et le partage continus des ressources en matière d'éducation pour la sécurité de l'information. Le NCISSE encourage les établissements d'enseignement à organiser des cours appropriés sur la sécurité des systèmes d'information dans le cadre de divers programmes afin de répondre aux besoins des consommateurs du XXI^e siècle et à proposer des cours répondant à la demande croissante de spécialistes en sécurité des systèmes d'information.

Lors de sa réunion annuelle de 1998, le NCISSE a produit un programme d'action très vaste résultant des contributions de ses divers participants. Ce programme comprend des efforts à entreprendre par le secteur public, le secteur privé et les établissements d'enseignement supérieur, à la fois individuellement et en coopération les uns avec les autres.

L'une des actions communes les plus importantes qui sont nécessaires est la clarification des connaissances, des compétences et des attitudes définissant un spécialiste de la sécurité de l'information, afin de permettre la formulation de normes précisant ce que les spécialistes de la sécurité de l'information devraient connaître et être capables de faire. Étant donné que la sécurité de l'information n'en est elle-même qu'aux premiers stades de la formation d'une discipline autonome, il nous faut identifier les « meilleures pratiques » actuelles pour les inclure dans des normes professionnelles d'une façon qui permette une évolution continue. Enfin, les trois éléments constitutifs du Colloque doivent surmonter la résistance aux normes de la part du personnel travaillant dans le secteur de la sécurité de l'information parce que l'on attend de toute profession le respect de la discipline incorporée dans les normes.

Le Colloque présenta également des recommandations générales d'action pour le secteur privé en affirmant que le secteur industriel doit fournir aux établissements d'enseignement des crédits, du matériel et des logiciels, et contribuer à l'entretien des systèmes d'information sur les campus des universités; fournir une formation

sur le tas aux membres du personnel enseignant, y compris à ceux qui ne travaillaient pas auparavant dans le secteur de la sécurité de l'information; et financer des bourses pour les étudiants qui désirent travailler dans ce domaine.

Le NCISSE demanda au gouvernement de formuler et de partager des programmes de cours en sécurité de l'information, et d'encourager le développement de Centres universitaires pour la protection de l'infrastructure sur le modèle des Centres des matériaux constitués sous l'égide de la « National Science Foundation » et des Centres des transports constitués sous l'égide du ministère des transports.

Les membres du Colloque demandèrent aux spécialistes en sécurité de l'information dans tout le pays d'encourager les discussions entre les membres du personnel enseignant, d'organiser plus de conférences sur la sécurité de l'information, de créer plus de sites Web et de publier plus de revues scientifiques sur la protection des réseaux d'information américains. Ils soulignèrent également le besoin d'établir un système officiel de récompense pour les meilleurs programmes d'enseignement sur la sécurité de l'information.

Le NCISSE encouragea également les établissements d'enseignement supérieur à augmenter le nombre de programmes contenant des cours sur la sécurité de l'information et à inclure des cours sur la sécurité dans les programmes obligatoires pour tous les étudiants.

L'inclusion de programmes d'enseignement traitant les questions éthiques et culturelles posées par les systèmes modernes d'information est particulièrement importante. Ceci concerne des thèmes tels que la préservation des valeurs traditionnelles dans l'ère moderne de l'information et la manière dont elles devront peut-être s'adapter.

Comme de nombreuses valeurs éthiques et culturelles sont formées très tôt dans la vie, les établissements d'enseignement supérieur sont encouragés à développer des programmes de sécurité de l'information en collaboration avec l'éducation secondaire.

Reconnaissant le fait que l'enseignement supérieur lui-même constitue une profession guidée par des normes, le Colloque encouragea les établissements

d'enseignement supérieur à demander conseil à des organismes d'accréditation pour le placement approprié de la sécurité de l'information dans leurs programmes d'enseignement.

Enfin, étant donné que l'éducation est une préoccupation qui dure toute la vie dans une société technologique en évolution rapide, l'enseignement supérieur fut encouragé à fournir des programmes d'éducation continue pour les spécialistes en sécurité de l'information qui travaillent déjà dans ce secteur. Le Colloque recommanda aux éducateurs en sécurité de l'information de développer et de partager des exercices de travaux pratiques en laboratoire en sécurité de l'information, de concevoir des jeux informatiques qui expriment des valeurs appropriées pour un personnel responsable et compétent en informatique, de prévoir des endroits où partager des documents pédagogiques et de rédiger plus de manuels d'enseignement, en particulier sur les questions pratiques. Le programme d'action du NCISSE demande également aux experts en enseignement du droit d'aider les juristes américains à comprendre la sécurité de l'information.

DES MÉTHODES D'INSTRUCTION BASÉES SUR INTERNET

Le besoin national critique de spécialistes en sécurité de l'information est caractéristique du monde technologique moderne. Comme la technologie change rapidement, ces spécialistes doivent s'engager à un recyclage permanent leur permettant de toujours renouveler et développer leurs connaissances. Et tous ces spécialistes doivent être prêts à réorienter leur carrière et à acquérir de nouvelles compétences au fur et à mesure que les changements de la technologie entraînent des modifications des besoins de personnel.

Le besoin de spécialistes en sécurité de l'information a considérablement augmenté au cours des dernières années. Cette demande de spécialistes qualifiés a entraîné à son tour une demande de débouchés en éducation pour produire de nouveaux spécialistes et pour réorienter la carrière des spécialistes actuels dans une nouvelle direction. Mais il ne serait pourtant pas raisonnable de s'attendre à ce que ces spécialistes intéressés par l'éducation continue interrompent leur carrière et suspendent leur vie familiale pour suivre des

cours traditionnels sur un campus universitaire. C'est pour cette raison le besoin d'éducation continue pour des spécialistes adultes qui ne perturbe pas leur vie familiale ou professionnelle que l'on constate un tel intérêt pour l'éducation au moyen d'Internet. L'université James Madison a répondu à ce besoin et à la technologie Internet en proposant un programme d'enseignement spécialisé de troisième cycle en sécurité de l'information sur Internet.

Le programme est proposé en tant que programme d'enseignement sur Internet par le biais de contrats avec des organisations qui peuvent assurer l'intégrité des procédures d'examens pour leurs collaborateurs.

Le programme se compose de 13 cours de sept semaines chacun, et il nécessite un peu plus de deux ans de travail. Un groupe d'étudiants formant une « cohorte » commence le programme, suit les 13 cours dans l'ordre et termine le programme ensemble.

Le programme d'enseignement sur Internet combine un projet d'étude indépendant avec un enseignement dirigé et du travail en groupe coordonné par un établissement central qui fournit un réseau de services. Les professeurs et la technologie fournissent un système de transmission des connaissances respectant des normes académiques élevées d'une façon très souple qui tient compte des besoins des participants. Des groupes de discussion sur Internet examinent, discutent et évaluent de manière critique les concepts de la sécurité de l'information. Chaque cours consiste en une séquence de cours théoriques et de problèmes à résoudre.

Les présentations des concepts par Internet peuvent être vues depuis n'importe quel point d'accès à Internet, où que ce soit dans le monde, et quand on le désire. Dans chaque classe, les projets proposent une orientation pratique explicitant les concepts et les documents étudiés.

LE PROGRAMME DE SÉCURITÉ INFORMATIQUE À L'UNIVERSITÉ JAMES MADISON

Les participants qui achèvent le Programme de sécurité de l'information à l'université James Madison obtiennent une maîtrise ès sciences informatiques avec spécialisation en sécurité de l'information. Le

programme est basé sur une norme sanctionnée par la L'Agence de la sécurité nationale (« National Security Agency»), et il est conçu pour développer les connaissances et les compétences nécessaires pour comprendre les rapports entre la sécurité de l'information et la technologie de l'information, et pour mettre en corrélation les aspects techniques et humains de ces deux disciplines.

Les cours administrés par le personnel enseignant de l'université James Madison portent essentiellement sur l'administration, la gestion, l'évaluation et la mise en œuvre de la technologie informatique, en attachant une importance particulière à la sécurité de l'information. La gestion des programmes de sécurité de l'information comprend la préservation et la protection de la confidentialité, de l'intégrité, de la disponibilité, de l'authenticité et de l'utilité de l'information dans des limites de risques acceptables.

Les membres du programme, qui travaillent en équipes :

- développent les connaissances et les compétences nécessaires pour comprendre les rapports entre la sécurité de l'information et les progrès technologiques des systèmes d'information afin de pouvoir mettre en place des programmes de protection et de détection des crimes ;
- développent des compétences très pointues requises pour des postes techniques, d'encadrement, de choix politiques et autres dans les domaines de la sécurité de l'information et de la technologie informatique en ce qui concerne l'évaluation des vulnérabilités, des menaces et des risques ;
- acquièrent les perspectives nécessaires pour des analystes, directeurs, administrateurs et praticiens de la sécurité de l'information afin de leur permettre de planifier, d'évaluer et de mettre en œuvre les techniques et programmes de sécurité de l'information ;

- mettent en corrélation les aspects techniques et humains de la sécurité de l'information et de la technologie informatique en ce qui concerne la protection des systèmes d'information ;

- développent des compétences fondamentales en conception de bases de données et de systèmes d'information, de systèmes d'exploitation et de réseaux, ainsi qu'en formulation de logiciels d'application pour améliorer la prévention des crimes et augmenter les responsabilités dans le cadre des enquêtes.

Le programme commence par une phase préparatoire pour les personnes qui ont besoin de renforcer leurs compétences en informatique avant de commencer les cours fondamentaux dans ce domaine. Cette phase préparatoire est suivie de trois cours en informatique qui traitent la gestion des bases de données, les systèmes d'exploitation et les réseaux, et le développement de logiciels d'application. En s'appuyant sur cette fondation très solide, la troisième période introduit la sécurité de l'information, les concepts de systèmes d'information sécurisés et les techniques de stockage et de transmission sans risque de l'information, notamment par encodage. Le quatrième module concerne les questions de gestion et d'administration en matière de sécurité de l'information, y compris l'analyse des risques et des vulnérabilités, les outils et procédures de contrôle des systèmes d'information, et les questions juridiques, éthiques et politiques. Le dernier projet du programme intègre tout ce qui a été appris en demandant aux participants d'analyser la sécurité d'un système d'information. ●

LE PROGRAMME D'ÉTUDE DE LA SÉCURITÉ DE L'INFORMATION À L'UNIVERSITÉ JAMES MADISON

Le programme d'étude de la sécurité de l'information à l'université James Madison comprend les cours suivants, divisés en plusieurs modules :

1. Module d'informatique fondamentale

Systèmes d'exploitation et réseaux – Concepts et principes des systèmes d'exploitation à utilisateurs multiples. Mémoire, unité centrale, affectation des dispositifs d'E/S (entrée/sortie), ordonnancement et sécurité. Hiérarchies de mémoires, évaluation des performances, modèles analytiques, simulation, programmations concurrentes et processeurs parallèles.

Systèmes de gestion de bases de données – Types de stockage physique et méthodes d'accès; modèles de données; algèbre et calcul relationnels, et langages de définition et de consultation; dépendances, décomposition et normalisation; conception de bases de données; récupération; homogénéité et concurrence; bases de données distribuées. Exemples de bases de données commerciales.

Développement de logiciels d'applications – Cycle de développement des logiciels, gestion des projets de logiciels, outils et méthodes de développement, assurance qualité des logiciels, modèles de langages de programmation et emploi de ceux-ci dans le cadre du développement de logiciels.

2. Module technique sur la sécurité de l'information

Introduction à la sécurité de l'information – Aperçu des menaces aux systèmes de sécurité de l'information, responsabilités et outils élémentaires pour assurer la sécurité de l'information et pour les domaines de la formation, et des priorités nécessaires au sein des organisations pour atteindre et maintenir un degré élevé de sécurité.

Systèmes sécurisés – Définition d'un « système sécurisé » et considérations relatives à la conception, l'évaluation, la certification et l'accréditation des systèmes sécurisés, y compris des considérations relatives au matériel et au logiciel, telles que les contrôles du développement, la validation/vérification, la distribution assurée et d'autres questions d'assurances. Mise en œuvre, gestion des configurations et administration des systèmes sécurisés. Importance de la compréhension de la psychologie et du modus vivendi de l'attaquant intelligent afin de formuler et d'entretenir une défense puissante.

Cryptographie – Ce cours permet à l'étudiant de comprendre les principaux protocoles d'encodage et de pouvoir les mettre en pratique. Il traite la conception et l'analyse des systèmes qui protègent les communications ou résistent à l'analyse cryptographique.

3. Module de gestion de la sécurité de l'information

Vulnérabilité, risques et analyse des systèmes d'information – Les vulnérabilités et risques inhérents au fonctionnement et à l'administration des systèmes d'information sont identifiés et explorés.

Contrôles de la sécurité de l'information – Les étudiants formulent des plans et effectuent un contrôle de la sécurité de l'information comprenant un examen matériel approfondi de la sécurité. Ils formulent et mettent en œuvre des normes permettant de surveiller les activités normales d'un système d'information.

Politiques, procédures, questions de droit et déontologie – Développement, évaluation et mise en œuvre de politiques et de procédures administratives de sécurité dans un système UNIX situé dans un environnement sécurisé. Préparation d'un Guide administratif de sécurité ou d'une annexe pour un tel document.

4. Projet final sur la sécurité de l'information

Un projet final intègre l'ensemble du programme en demandant aux participants d'analyser la sécurité d'un système d'information, d'examiner et d'analyser l'efficacité des options disponibles pour améliorer cette sécurité, de passer en revue le contexte juridique et éthique plus général de ces options, et de sélectionner et de proposer une procédure de mise en œuvre pour l'une de ces options.

Cours préparatoires – Les étudiants qui ne sont pas prêts à commencer l'étude des documents fondamentaux peuvent s'inscrire pour une séquence préparatoire de trois cours: étude élémentaire accélérée de la programmation des ordinateurs; étude approfondie de la programmation des ordinateurs; et étude élémentaire accélérée des systèmes informatiques.

LES SECTEURS PUBLIC ET PRIVE ONT INTERET A PARTAGER LEUR EXPERTISE DANS LE DOMAINE DE LA SECURITE

*Entretien avec M. Howard Schmidt
Directeur de la sécurité informatique chez Microsoft*

Le gouvernement et un grand nombre d'entreprises privées ont maintenant les moyens de se contacter et de se soutenir en cas d'attaque de leurs systèmes informatiques et autres infrastructures clés, déclare M. Howard Schmidt, directeur de la sécurité informatique chez Microsoft. M. Schmidt fait état de l'importante coopération qui existe entre les sociétés face au risque de cyberguerre. « Quand il s'agit de problèmes de sécurité, il y a peu de cas dans lesquels la concurrence intervient, affirme-t-il. Nous collaborons avec nos concurrents comme avec nos partenaires pour aider à établir des normes afin de pouvoir tous parvenir à mettre au point et à garantir une bonne sécurité. » M. Schmidt était interviewé par Dian McDonald, directrice de la rédaction.

QUESTION : Comment évaluez-vous la vulnérabilité des infrastructures clés des Etats-Unis face à une attaque cybernétique? Sommes nous prêts à faire face à ce genre d'attaque?

M. SCHMIDT : Mon évaluation cadre assez bien avec celle de la Commission présidentielle sur la protection de l'infrastructure de base, à savoir que nous avons du travail à faire dans ce domaine. Ce sont des problèmes qui, lorsque la commission a été établie, n'étaient pas au premier plan des préoccupations. En ce qui concerne notre capacité de surmonter de telles attaques, je crois que la Commission présidentielle sur la protection de l'infrastructure de base a beaucoup aidé à mettre les secteurs public et privé en mesure de faire face collectivement à ce genre d'attaque. Ces secteurs font du bon travail pour répondre à cette menace.

Q : Collaborez-vous avec la Commission?

M. SCHMIDT : Oui, nous travaillons avec elle. Nous avons fait venir ses membres ici (à Redmont, Etat de Washington) pour deux réunions. Je me suis rendu moi-même à Washington pour assister à deux réunions. En fait, nous sommes en train d'organiser la réunion d'un nombre important de représentants du gouvernement et du secteur privé pour qu'ils parviennent à un accord sur la façon d'améliorer l'infrastructure.

Q : Quels sont les changements structurels auxquels votre société a procédé en raison de ces nouvelles menaces pour la technologie?

M. SCHMIDT : Permettez moi de formuler différemment votre question, parce que nous ne les considérons pas comme des menaces pour la technologie, mais comme l'utilisation de la technologie pour donner à quelqu'un la possibilité de s'attaquer à un vaste auditoire, si je puis dire. A la base, c'est ainsi que nous voyons le problème. Ce genre de menace est ancien, mais la technique utilisée est plus moderne. Pour y répondre, nous avons mis sur pied, il y a un an, un programme dont nous sommes très fiers: le MIAP ou Microsoft Information Assurance Program, qui nous permet d'unir un grand nombre d'éléments internes qui se rapporteraient à la protection de l'information ou assureraient la validité de notre information. Nous avons actuellement un organisme qui chapeaute plusieurs programmes et fonctions, y compris un plan de relèvement après un désastre, un système de conservation et de classement des données, une stratégie de secours, le groupe chargé de la sécurité lui-même, le groupe chargé de la sécurité du matériel en rapport avec la protection de l'information ainsi que le groupe chargé de la sécurité des produits, étant donné que Microsoft fabrique des logiciels.

Dans le cadre de cette structure, nous procédons à des échanges entre toutes les spécialités, non seulement pour sécuriser l'information et les systèmes, mais pour garantir que les produits que nous mettons au point bénéficient de l'expérience des experts de la sécurité de l'information afin d'aider à améliorer ces produits.

Q : En ce qui concerne les stratégies permettant de faire

face à la cyberguerre, dans quelle mesure collaborez-vous avec les autres sociétés?

M. SCHMIDT : Nous le faisons dans une très large mesure. En fait, nous avons plusieurs groupes différents, par exemple l'Association pour la sécurité des systèmes d'information, organisation sans but lucratif dont les membres travaillent dans le domaine de la sécurité, des représentants de la Charles Schwab Company; de U.S. Space Alliance; Air Touch Cellular et de diverses agences gouvernementales. Nous assistons à des conférences et travaillons avec le Garter Group, grosse société de consultants en informatique. Nous participons à l'initiative de l'ancien sénateur Sam Nunn, qui a joué un rôle très important dans la protection de l'infrastructure. M. Nunn coordonne un forum périodique sur la sécurité au Georgia Institute of Technology, situé à Atlanta, et nous faisons aussi partie de ce forum.

Il y a donc beaucoup d'échanges d'information, de meilleures procédures dans les entreprises privées qui travaillent dans le domaine de la sécurité. Et il y a d'autres groupes comme le « Federal Computer Investigations Committee » et la « High Tech Crimes Investigators Association », composés de représentants des secteurs public et privé, et qui collaborent dans ce domaine. Nous avons donc d'excellentes relations et notre collaboration est très étroite.

Quand il s'agit de problèmes de sécurité, il y a peu de cas dans lesquels la concurrence intervient. Nous collaborons avec nos concurrents comme avec nos partenaires pour aider à établir des normes afin de pouvoir tous parvenir à mettre au point et à garantir une bonne sécurité.

Q : Pouvez-vous nous donner des détails sur la façon dont votre société coopère avec le gouvernement face aux nouveaux dangers qui pèsent sur les systèmes informatiques?

M. SCHMIDT : Nous suivons plusieurs voies. Evidemment, les gens qui conçoivent les produits que nous utilisons tous ont des contacts très étroits avec les fonctionnaires de toutes les agences gouvernementales pour faire en sorte que leurs produits répondent à la nécessité d'assurer la sécurité de l'infrastructure de base, responsabilité qui incombe au gouvernement.

D'un autre côté, en tant que fournisseur de services en ligne, nous faisons nous mêmes partie de l'infrastructure et travaillons très étroitement, par exemple, avec les personnes qui procèdent à des enquêtes en ligne, pour leur fournir l'expertise technique dont elles ont besoin. Nous avons maintenant un téléphone rouge qui est mis vingt quatre heures sur vingt quatre, sept jours par semaine, à la disposition de la police pour les enquêtes dont font l'objet les personnes qui se livrent à des activités illicites sur Internet.

Nous tenons également des réunions périodiques pour améliorer nos procédures. Nous faisons fréquemment des exposés à des groupes de fonctionnaires. C'est ainsi qu'il y a quelques mois, j'ai prononcé le discours principal à la « National Defense University », à Washington. J'ai assisté à la conférence intitulée « Defending CyberSpace 98 », à Washington en septembre. Nous prenons part à ce genre de forum et partageons notre expérience mutuelle pour améliorer le travail de tous dans ce domaine.

Q : Pensez-vous que le gouvernement devrait jouer un plus grand rôle dans la protection des infrastructures clés et, dans l'affirmative, quel devrait être ce rôle, selon vous?

M. SCHMIDT : A la base, j'estime que le gouvernement devrait continuer à collaborer avec le secteur privé. Je pense que la Directive présidentielle 63 (PDD 63) qui a établi l'Office de protection de l'information de base, a posé de bonnes bases pour faciliter la collaboration entre le gouvernement et le secteur privé. Et je pense que grâce à ce rôle des pouvoirs publics, et sans qu'on ait besoin de nouvelle législation ou de nouveaux règlements, nous pouvons accroître notre coopération avec le gouvernement afin d'assurer la protection des infrastructures clés.

Q : Existe-t-il des conflits d'ordre philosophique aux Etats-Unis entre les besoins des entreprises en matière d'information et les préoccupations du gouvernement sur le plan de la sécurité?

M. SCHMIDT : Je ne vois, à la base, aucun conflit. Ce que nous constatons dans ce domaine, c'est que nous cherchons tous à assurer le maximum de sécurité tout en protégeant la confidentialité de l'information des

sociétés, de l'information gouvernementale et personnelle et des choses de cette nature. Donc, même s'il peut exister des divergences sur la façon dont nous abordons ces problèmes, ce qui est important, à mes yeux, c'est le fait que nous sommes tous d'accord sur la nécessité de collaborer pour assurer la protection de l'infrastructure.

Q : Comment le public et le secteur privé peuvent-ils améliorer leur collaboration pour mettre en place des moyens de défense efficaces contre le terrorisme ou autres actes d'hostilité?

M. SCHMIDT : Je pense que nous avons pratiquement fait le nécessaire dans ce domaine. En fin de compte, nous avons maintenant avec les différentes agences gouvernementales et un grand nombre de sociétés des moyens de nous contacter et de nous soutenir au cas où un événement de ce genre se produirait. Et je pense que nous sommes très bien placés pour fournir l'expertise technique nécessaire aux organes chargés de faire respecter la loi. Manifestement, nous sommes en train de mettre au point certaines des modalités permettant d'institutionnaliser et de formaliser ces procédures et c'est ce que nous allons continuer à faire de mieux en mieux.

Q : Comment Microsoft incorpore-t-il la sécurité dans ses produits pour aider ses clients à se protéger?

M. SCHMIDT : C'est une question qui n'entre pas dans mes compétences, mais ce que je peux dire, c'est que des représentants de Microsoft se réunissent régulièrement avec leurs clients. Nous avons tous des préoccupations en matière de sécurité. Les techniciens de Microsoft chargés de la mise au point des produits s'efforcent d'assurer à ces produits une meilleure sécurité et ils collaborent avec nous et avec les professionnels de la sécurité de l'information. Il y a donc une concertation constante, pour garantir la sécurité de nos produits non seulement maintenant, mais aussi à l'avenir, au cas où d'autres points vulnérables seraient découverts.

Q : Pensez-vous que les contrôles techniques actuels permettent de nous protéger des virus et des cyberterroristes?

M. SCHMIDT : On a beaucoup parlé, récemment, de différents types de virus et autres choses de ce genre. Manifestement, la réaction est la même que lorsque d'autres types d'activités illicites sont découvertes. Le secteur privé et le gouvernement collaborent pour les contrecarrer, pour nous mettre en mesure de faire face à de telles menaces et pour prédire ce que quelqu'un pourrait tenter de faire à l'avenir. Tant que nous partagerons les données et les excellents systèmes d'information sur lesquels nous comptons tous, il y aura des gens qui essaieront de perturber ces systèmes. Mais grâce à la technologie, à l'éducation et à la prise de conscience des risques, je pense que nous pouvons faire du bon travail pour résoudre tous les problèmes de protection qui s'y rapportent.

Q : Avez-vous mis au point des techniques qui protégeraient une société d'un déluge incessant de messages électroniques en provenance d'un cyberterroriste?

M. SCHMIDT : Oui. Un certain nombre de ressources, de mises à jour et de modifications de programmes sont incorporées dans nos produits, comme le font d'autres sociétés, pour remédier à ce genre de problème. De plus, dans le cadre de notre « Security Partners Program » (Programme des partenaires en sécurité), nous collaborons avec des sociétés qui ont mis au point d'excellents outils, j'entends par là des programmes informatiques qui aideraient vraiment à prévenir l'interruption de nos services par des attaques, des bombes électroniques et autres choses de ce genre. Nous avons fait de grands progrès dans ce sens. ●

ASSURER LA SECURITE DES SYSTEMES INFORMATIQUES

James Lingerfelt

Consultant principal chez IBM pour la sécurité publique et les affaires judiciaires

Les menaces qui pèsent sur les systèmes informatiques ne proviennent pas principalement du super pirate de l'informatique, affirme M. James Lingerfeldt, spécialiste des techniques et de la planification stratégique relatives à la répression de la criminalité. « En réalité, le plus grand danger pour les systèmes informatiques et les bases de données provient des sources dites sûres. » L'auteur estime qu'une évaluation réaliste des besoins et des menaces en matière de sécurité, débouchant sur l'élaboration et l'application consciencieuses d'un plan de sécurité, peut assurer une protection efficace contre la vaste majorité des menaces, et ce à un coût raisonnable.

Il identifie les domaines d'où émanent les menaces réelles les plus fréquentes et propose sept principes stratégiques devant guider l'élaboration de plans de sécurisation des systèmes informatiques.

Les organes assurant la justice et l'ordre public ont actuellement une occasion sans précédent d'appliquer les techniques de l'information à la modernisation de leurs opérations et à l'amélioration de leurs services. Ces milieux hésitent cependant à s'engager sur cette voie, car ils craignent qu'en remplaçant ou en complétant leurs systèmes fermés à ordinateur central par des ordinateurs personnels reliés en réseau, et en adoptant des procédures automatisées, ils ne s'exposent à des actes de piraterie. Le coût estimatif élevé de la protection d'un système informatique contre les intrusions, et les dommages susceptibles de résulter de la perte de données extrêmement sensibles, semblent justifier cette aversion pour le risque en dépit des avantages que présenterait l'adoption des nouvelles techniques.

Il est vrai qu'en raison de l'essor spectaculaire de ces techniques, les systèmes d'information, les équipements et les bases de données se trouvent plus fortement exposés à des attaques de pirates. Mais le super « hacker » redouté, fort de ses vastes connaissances informatiques, représente rarement la menace la plus grave. En réalité, le plus grand danger pour les systèmes informatiques et les bases de données provient des sources dites « sûres », qui agissent souvent sans que les organes de justice et de police accordent la moindre attention à la sécurité fondamentale de leurs systèmes d'information. Or, une évaluation réaliste des besoins et des menaces en matière de sécurité, débouchant sur l'élaboration et l'application sérieuses

d'un plan de sécurité, pourrait leur assurer une protection efficace contre la vaste majorité des menaces, et ce à un coût raisonnable.

PERCEPTION ET RÉALITÉ

Alors même que de nombreux organes de police engagent des dépenses financières substantielles dans de nouveaux outils informatiques, on constate une augmentation du nombre d'actes de piraterie contre leurs systèmes d'information. On observe de même une augmentation du nombre de plaintes faisant état d'utilisations illicites d'informations provenant des bases de données de la police, de vols d'information de la police, et de vols de matériel informatique appartenant à des services de police. La fréquence de ces rapports a découragé nombre d'organismes de police de se doter de systèmes autres que leurs systèmes fermés existants. Et pourtant, les nouveaux besoins fonctionnels des organes chargés de l'ordre public exigent d'eux qu'ils modifient les méthodes par lesquelles ils acquièrent, partagent et diffusent l'information.

Des changements opérationnels se sont imposés du fait de la nécessité de distribuer les informations hors de l'organisation ou d'échanger l'information avec des organismes extérieurs et des particuliers.

Certains organismes ont réagi en affectant du personnel à de nouvelles tâches, aux dépens des forces

disponibles sur le terrain. D'autres ont mis en place de nouveaux systèmes « autonomes » qui fournissent exclusivement les nouveaux services, sans les intégrer ni les relier de manière complémentaire aux systèmes classiques de l'organisme. Ceci ne fait qu'augmenter la complexité des opérations ainsi que les coûts des systèmes informatiques en personnel, en temps et en argent.

Comme il a été noté plus haut, les menaces internes provenant de sources considérées comme sûres font plus de dommages que les intrusions de l'extérieur. Plusieurs incidents de ce type ont été signalés :

- Un réseau entier a été contaminé par un virus provenant d'une disquette que la division de planification du département avait distribuée pour obtenir les réponses à un sondage.
- Le chef d'un service de renseignement avait collé sur son ordinateur une feuille de papier où il avait inscrit son nom d'utilisateur et son mot de passe avec des instructions détaillées sur les procédures d'entrée en ligne.
- Un haut fonctionnaire de police a vendu à des mafieux un dossier informatique contenant la description et les numéros des plaques minéralogiques de toutes les voitures de police banalisées.
- Un administrateur de réseau novice a établi dans un service de police un réseau qui assurait à chaque utilisateur des privilèges d'administrateur.
- Les programmeurs d'applications d'un important service de police ont été autorisés à utiliser, sans essais ni examen méthodiques, un nouveau code de programme qui, étant défectueux, a mis le système tout entier en panne pendant vingt quatre heures.
- Le gouvernement d'un Etat a établi un site Internet sans filtre sécuritaire. En l'espace de 24 heures, son fichier de code utilisateur et son mot de passe étaient affichés dans une téléconférence de pirates. Les autorités ont eu le mérite d'avertir d'autres Etats de leur mésaventure et leur ont évité de commettre la même erreur.

Pas un seul de ces cas n'implique de super pirate attaquant un système d'information officiel. Dans le dernier exemple, l'intrusion a été rendue possible par la plus grossière des erreurs, équivalant à laisser sa maison ouverte à tous les vents. Ces incidents auraient pu être évités par une planification, une formation ou une supervision élémentaires.

En résumé, il existe une menace accrue d'attaques de l'extérieur du fait de la prolifération des systèmes informatiques, mais les proportions elles mêmes n'ont pas changé : les parts du gâteau restent inchangées : c'est le gâteau lui même qui a grossi. Les menaces se sont elles multipliées ? Certes. Ont elles changé ? Non.

Le risque accru de piraterie informatique est dû à plusieurs causes :

- Les nouveaux modèles opérationnels : le secteur public imite le secteur privé, avec un retard d'environ cinq ans.
- L'essor exponentiel des systèmes informatiques : les ordinateurs et les réseaux se sont introduits dans pratiquement tous les domaines de notre existence.
- La diminution des coûts : les techniques d'aujourd'hui sont peu coûteuses. Quelles que soient les mesures utilisées, les coûts de base sont plus faibles qu'ils ne l'ont jamais été, et le coût des nouvelles techniques décroît plus rapidement qu'il y a encore quelques années en raison des progrès rapides et de la concurrence accrue.

LES NOUVEAUX MODÈLES OPÉRATIONNELS

Dans le processus de décentralisation des activités, le siège de l'organisme en tant que lieu central de prise de décisions et de rassemblement de l'information a été remplacé par des unités indépendantes périphériques soutenues par un système de distribution de l'information.

Dans la technologie de l'information, cette évolution se traduit par l'abandon progressif des systèmes à architecture fermée au profit de réseaux, intranets et extranets. La distribution de l'information pose des difficultés accrues pour la protection des équipements,

pour les opérations de surveillance et pour la solution des problèmes, du fait de la multiplication des points d'exposition. Du côté positif, la distribution électronique de l'information autorise des gains énormes de productivité, si bien que l'investissement consenti devient souvent rentable en moins d'un an.

Le secteur privé commence à mettre l'accent sur les fonctions de base au lieu d'essayer de tout fournir à tout le monde. Les entreprises ont à présent des effectifs beaucoup plus modestes, ce qui leur permet de résoudre les problèmes de main d'œuvre et d'éviter les problèmes logistiques liés aux mutations. Seuls sont pourvus les postes qui contribuent directement à l'accomplissement des objectifs de l'entreprise. La pratique des fusions et des acquisitions impose fréquemment le recours à des services extérieurs pour remplir les fonctions administratives et d'appui, en particulier celles liées à l'information. Les organes judiciaires (et le gouvernement tout entier) se sont engagés sur la même voie de la rationalisation des opérations, de la réduction des coûts et de l'amélioration des services.

En outre, il est devenu très difficile de conserver un personnel technique compétent. Les organismes publics ne sont pas en mesure de concurrencer le secteur privé sur le plan des salaires pour remplacer les transfuges et cette réalité a également accru l'utilisation de services extérieurs.

Le renouvellement accéléré des cadres et des gestionnaires est lui aussi, aujourd'hui, une réalité de la vie des organisations. La pratique des compressions de personnel et des raids des entreprises chez leurs concurrentes pour leur ravir leurs meilleurs éléments, entraîne le danger de voir les cadres supérieurs ou intermédiaires emporter avec eux des biens intellectuels importants. C'est ainsi qu'un gestionnaire a été poursuivi et condamné pour ce type d'infraction lorsqu'il s'est avéré que l'organisation du répertoire de fichiers informatiques de son nouvel employeur était absolument identique à celle de l'entreprise qu'il avait quittée. Fait rarement publié ou même admis, les sociétés qui réduisent leurs effectifs subissent souvent des millions de dollars de pertes en matériel, en logiciel, en fournitures et en équipement si les employés visés reçoivent un préavis de licenciement.

En dépit des avantages de la formule, l'appel à des services extérieurs peut mettre en cause la sécurité informatique. Il est donc particulièrement important d'appliquer un plan de sécurité lorsque des responsabilités essentielles à l'accomplissement de la mission sont confiées à des employés contractuels ou à des sous traitants extérieurs. L'organisme peut exiger que tous les contractuels fassent l'objet de vérifications des antécédents et des références.

LA CROISSANCE EXPONENTIELLE DE L'UTILISATION DE LA TECHNOLOGIE DE L'INFORMATION

L'informatique et les réseaux électroniques se sont insinués dans pratiquement tous les domaines de notre existence. Les fraudes, les vols, la divulgation illicite d'informations sont rendus possibles par les ordinateurs, les réseaux et l'internet que nous utilisons. Nous assistons à l'apparition de nouvelles formes de délits et à la réapparition de vieilles combines.

Heureusement, l'utilisation croissante des ordinateurs a permis de faire progresser les techniques, les normes et l'identification des meilleures pratiques. La technologie a profité des enseignements tirés des erreurs, ce dont nous avons tous bénéficié aussi. Les pratiques relatives à la sécurité se sont également améliorées grâce aux leçons apprises, qui ont permis de dégager un ensemble de principes pratiques. Le secteur privé a préparé la voie dans ce domaine. La plupart des nouveaux produits (matériel et logiciel) ont maintenant des fonctionnalités de sécurité incorporées. Qu'elles soient utilisées ou non est une autre question.

LA DIMINUTION DES COÛTS

Quelles que soient les mesures retenues, le coût des techniques informatiques de base est plus bas qu'il ne l'a jamais été. Pratiquement tout le monde peut se permettre un ordinateur.

L'équipement coûte moins cher, d'une part, mais les sommes inscrites aux budgets des organismes publics pour réaliser des investissements dans ce domaine sont aussi plus généreuses aujourd'hui qu'à n'importe quel moment depuis la fin des années 1960 et le début des années 1970. C'est ainsi, par exemple, que le

financement des initiatives relatives au passage informatique à l'an 2000 et à la criminalité informatique se chiffre en milliards de dollars, et qu'il vise spécifiquement à améliorer ou à remplacer les systèmes d'information du secteur public. C'est là l'occasion rêvée pour les organes judiciaires d'inclure la sécurité dans l'élaboration et l'adoption de nouveaux processus opérationnels et de systèmes informatiques. La mise à niveau des systèmes de sécurité après coup est une opération trop onéreuse et généralement peu efficace.

LA PLANIFICATION DE LA TECHNOLOGIE DE L'INFORMATION

Le livre de science fiction « Le guide de l'autostoppeur galactique » a pour première règle : ne pas paniquer.

Ce conseil s'applique également à la planification de la sécurité informatique. Un grand nombre d'organismes hésitent à investir dans les systèmes informatiques car ils s'imaginent, croyance tenace et exagérée, que les réseaux seront immédiatement assiégés par les pirates et envahis par les intrus.

En dépit de l'accroissement des risques d'intrusion, les compétences et les outils nécessaires pour construire des défenses efficaces sont déjà disponibles et s'améliorent quotidiennement. Une planification préalable efficace permet de répondre rapidement et de manière appropriée à n'importe quelle attaque, de prévenir la plupart d'entre elles et de minimiser l'impact des autres.

La planification des systèmes d'information doit s'inscrire dans une perspective large tenant compte de tous les aspects des activités de l'entreprise : le plan doit découler directement des plans opérationnels de l'organisation. Il doit décrire les exigences relatives aux activités destinées à réaliser les buts opérationnels et non pas être une liste idéale et illimitée des composantes de systèmes. On s'attachera donc avant tout à définir l'objectif visé et non pas la manière de l'atteindre. Il existe généralement de multiples manières de répondre aux exigences, avec des variations considérables au niveau des coûts. Chaque dollar dépensé doit être clairement justifié. Et la sécurité doit être intégrée dans le plan dès le stade de la conception.

On adoptera une charpente de système aussi simple que possible, car la simplicité constitue un atout majeur pour la sécurité. Les systèmes multiples, quel que soit leur degré d'intégration, présentent de multiples points d'accès et nécessitent de multiples systèmes de sécurité et d'appui qui se traduisent par des augmentations de coûts.

LES SEPT PRINCIPES STRATÉGIQUES RELATIFS À LA SÉCURISATION DES SYSTÈMES INFORMATIQUES

1. LA SIMPLICITÉ AVANT TOUT. Si le dispositif de sécurité est trop compliqué, les utilisateurs évitent de s'en servir ou essaient de le contourner, ce qui le rend inopérant ou en réduit l'utilité. Les mesures de sécurité moderne peuvent être efficaces et discrètes.

2. DÉFINIR À L'AVANCE LES RÈGLES, PROCÉDURES ET PÉNALITÉS. Ces trois éléments de la sécurité doivent être définis en fonction des besoins des utilisateurs, de la nature des applications et de l'information à protéger. Ils doivent aussi être strictement respectés. Il vaut mieux ne pas avoir de système de sécurité que de l'appliquer à moitié.

3. FORMER LE PERSONNEL À L'UTILISATION DU DISPOSITIF EN SOULIGNANT LES TROIS ÉLÉMENTS SUSMENTIONNÉS. On renforcera la formation en analysant et en diffusant des nouvelles pertinentes, telles que des articles sur les cyberattaques ou les usages abusifs des systèmes.

4. UTILISER AUTANT QUE POSSIBLE LES PRODUITS DISPONIBLES TELS QUELS DANS LE COMMERCE, PLUTÔT QUE DE DÉVELOPPER DES APPLICATIONS DE SÉCURITÉ SPÉCIALISÉES. Ceci est à conseiller pour plusieurs raisons, parce que les besoins des organisations sont relativement simples. Les organes judiciaires établissent des relations entre les personnes, et entre les personnes et les événements, en recueillant et en partageant les informations. Les produits standard basés sur des normes ouvertes ont été testés et ont fait leurs preuves ; leurs utilisateurs peuvent nous fournir des renseignements supplémentaires dont nous pouvons tirer des leçons. Même pour les nouveaux produits, on peut évaluer les méthodologies utilisées dans les tests et analyser les résultats. Et surtout, les

produits standard sont généralement bien documentés pour les utilisateurs et pour les techniciens. La documentation et les tests de sécurité sont fréquemment négligés lorsque l'on développe des applications spécifiques de manière interne.

5. TRIER L'INFORMATION, LES ÉQUIPEMENTS ET LES UTILISATEURS. PROTÉGER L'INFORMATION ET LES AVOIRS EN FONCTION DE LEUR VALEUR. L'information confidentielle doit être hautement protégée. En revanche, l'information publique ou facilement remplaçable ne nécessite pas une sécurité compliquée. Une évaluation objective démontrera que la part des éléments d'information publique est bien plus grande que celle des données confidentielles.

De même, les équipements (ordinateurs personnels, serveurs, câbles, ordinateurs centraux, etc.) et les fournitures (logiciels, disquettes, etc.) doivent être inventoriés et protégés de manière appropriée. Les organismes reçoivent souvent de grandes quantités de matériel et de logiciel (ordinateurs personnels, moniteurs, cartes de réseau, ordinateurs centraux, routeurs, etc.) sans inscrire les articles dans une base de données de contrôle des avoirs et sans les vérifier soigneusement pour s'assurer qu'ils ont bien reçu les articles commandés, que le matériel est bien configuré et qu'il fonctionne correctement. Ils n'ont donc pas de preuves à présenter en cas de perte des avoirs ou de difficultés de fonctionnement. La gestion de l'inventaire est une première étape. La deuxième étape est le contrôle de la configuration.

Au moment de la livraison, la configuration de chaque dispositif matériel doit être établie et chaque programme doit être enregistré selon les règles. L'inventaire contiendra alors une description détaillée de chacun des composants du système, matériel et logiciel, et du lieu où ils se trouvent (jusqu'au numéro du bureau et à son emplacement précis dans le bureau). Ces renseignements sont d'une grande valeur pour la protection des avoirs, pour l'identification des vols ou des intrusions, et lors des enquêtes en cas de problèmes. Il existe des logiciels qui vérifient la configuration et signalent automatiquement les problèmes aux administrateurs de la sécurité. Ils maintiennent également un journal des modifications et de la maintenance du système. Il est important que

les réparations effectuées, les améliorations apportées aux systèmes et les opérations de maintenance soient enregistrées. Enfin, des dispositifs physiques et des vis spéciales pour verrouiller les postes de travail peuvent réduire les vols et les modifications. Le règlement intérieur doit exiger que toute anomalie soit signalée et fasse l'objet d'une enquête.

Le tri des fournitures et des avoirs permet de leur accorder un traitement approprié selon leur coût ou leur importance pour la mission. Ce point est très souvent négligé. C'est ainsi que l'on conserve sous clé des fournitures bon marché telles que les disquettes alors que des biens essentiels tels que les serveurs ne sont pas protégés, se trouvent dans des bureaux ouverts, et que les câbles de réseau et les routeurs sont placés le long des plinthes des murs au lieu d'être protégés sous conduits et cachés dans les plafonds.

Il faut également trier les utilisateurs, à savoir contrôler les applications et les informations auxquelles ils ont accès et comment ils y ont accès. (Par exemple, un utilisateur donné peut avoir accès à un fichier réservé uniquement à partir de certains postes de travail et à certains moments). Il faut contrôler qui a le droit de créer des comptes ou d'établir des identifications d'utilisateurs dans un système, et opérer des vérifications fréquentes pour détecter les identités ou les comptes factices.

L'organisme doit être doté de bonnes capacités d'audit.

Un défaut de la cuirasse fréquemment négligé se situe au niveau de la documentation des systèmes. La documentation de tout genre est souvent traitée sans précautions et les classeurs sont laissés ouverts dans des bureaux accessibles au premier venu. Les détails techniques et les informations concernant les utilisateurs doivent être protégées. Il peut sembler plus pratique et moins coûteux de préparer et de publier une documentation « à tous usages », mais ceci présente des dangers. Les manuels d'utilisateurs finaux largement distribués contiennent souvent de grandes quantités d'informations techniques inutiles pour l'utilisateur, mais de grande valeur pour les pirates. Un pirate armé d'informations détaillées peut attaquer un système avec une précision scientifique au lieu de recourir à la force brute plus facilement détectable. On veillera donc à ne distribuer la documentation que

selon le principe du besoin de savoir.

La documentation doit être protégée, son accès contrôlé, et les utilisateurs doivent être formés aux méthodes à appliquer pour la protéger. La publication électronique de la documentation sur le réseau est recommandée, de préférence à son impression sur papier : elle réduit les coûts, simplifie les mises à jour et permet d'assurer une meilleure protection.

6. ETRE RÉALISTE AU SUJET DE L'ADMINISTRATION DE LA SÉCURITÉ. Il ne faut pas s'attendre à ce que les organes judiciaires, par exemple, puissent établir ou administrer un programme de sécurité impénétrable. Il faut tenir compte de manière réaliste des besoins de sécurité au regard des coûts et déterminer le niveau de soutien nécessaire pour réaliser les objectifs visés. On confiera donc aux employés les tâches qu'ils peuvent accomplir de manière efficace et les autres tâches à des sources extérieures. L'objectif global est d'obtenir les résultats définis par le plan de sécurité de l'information.

Un grand nombre de ressources sont disponibles pour satisfaire aux besoins de sécurité. Les services extérieurs constituent une solution efficace par rapport au coût. A mesure qu'augmente la dépendance à l'égard de l'informatique, l'importance attachée à la sécurité va également croissant et le secteur privé réagit en offrant des services de sécurité de grande qualité.

Une autre possibilité intéressante est celle du recours aux ressources que peuvent se fournir mutuellement les organes judiciaires et les spécialistes de la sécurité. Le partage des ressources, la mise en commun de fonds pour des acquisitions conjointes, les dons de services de la part des universités ou de la collectivité sont toutes des manières possibles de combler les lacunes du plan de sécurité.

7. TESTER, AUDITER, INSPECTER LES SITES ET FAIRE DES ENQUÊTES CONTINUELLES ET RANDOMISÉES. On utilisera une méthodologie d'examen et de tests des codes pour bloquer les entrées dérobées dans le système. On se servira de programmes automatiques d'audit et de surveillance, ainsi que de programmes qui vérifient les modifications des fichiers. On élaborera et on utilisera des programmes « avertisseurs » pour identifier les auteurs d'attaques

contre le système existant ou en puissance. On fera connaître les menaces et les ripostes. Il est particulièrement important de prendre des décisions rapides, cohérentes et appropriées en cas de violations détectées ou rapportées et de publier largement les mesures disciplinaires prises pour garantir la sécurité de l'information.

LES TECHNIQUES NOUVELLES

La sécurité des systèmes d'information a progressé aussi rapidement que tous les autres aspects de l'informatique, mais elle ne peut pas être efficace si le dispositif n'est pas déployé correctement. Pratiquement toutes les applications standard disponibles dans le commerce comportent des fonctions de sécurité. Les filtres sécuritaires sont plus robustes, plus adaptables et plus faciles à utiliser que jamais et à des prix très raisonnables. Les programmes de cryptage sont plus puissants et plus faciles à exécuter et à entretenir. La capacité de gérer et de surveiller les systèmes distribués à partir d'un point unique du réseau s'accroît constamment. Les programmes de surveillance et d'audit automatisés pour contrôler l'utilisation du système et alerter les administrateurs en cas d'atteinte ou de tentative d'atteinte à la sécurité arrivent rapidement à maturité.

L'un des domaines techniques où les progrès sont les plus prometteurs est la biométrie, qui permet d'identifier les individus d'après des caractéristiques physiques spécifiques (empreintes digitales, voix, géométrie de la main, empreintes rétiniennes, etc.). Les dispositifs biométriques permettent une authentification des utilisateurs plus efficace que jamais et empêchent les personnes non autorisées d'accéder à un système même si elles possèdent le mot de passe.

IBM, en coopération avec la Banque Barclays en Europe, effectue des essais de clavier de poste de travail à lecteur d'empreintes digitales. Les utilisateurs doivent se faire authentifier avant de pouvoir accéder à une partie quelconque du système. La technologie flash (algorithme de recherche d'images) est rapide et précise. Elle permet de rechercher dans une base de données de millions de fichiers (y compris d'images d'empreintes digitales) pour déterminer s'il existe une concordance. Cette technologie, alliée à l'usage de

réseaux à haute vitesse, se prête aux applications dans les GAB (guichets automatiques de banque) et autres dispositifs de transactions électroniques. Elle est utilisée actuellement au Pérou dans un système d'inscription sur les listes électorales à base d'empreintes digitales ; ce projet, qui a donné d'excellents résultats, contribuera à prévenir les fraudes électorales.

A mesure que ces techniques continueront d'évoluer, la sécurité de l'information continuera de s'améliorer sur les plans tant de l'efficacité que de la facilité d'utilisation. ●

PERILS ET POTENTIALITES DE LA GUERRE INFORMATIQUE

James Adams
Président-directeur général d'« Infrastructure Defense, Inc. »

« J'ai le pouvoir, les moyens, assis chez moi, muni de mon ordinateur et de mon modem... de faire la guerre. C'est un environnement très différent de tout ce que nous avons pu connaître par le passé. » C'est ce qu'affirme M. James Adams, directeur d'« Infrastructure Defense, Inc. », centre d'échange d'informations et de décisions relatives à l'infrastructure de base au sein du secteur privé ainsi qu'entre les secteurs public et privé dans le monde entier. L'article qui suit est l'adaptation d'un discours prononcé par M. Adams à l'Agence d'information des Etats-Unis en août 1998.

L'armée américaine a organisé l'année dernière un exercice comportant la simulation suivante : une crise internationale se prépare, et une puissance étrangère engage trente cinq « pirates » informatiques pour neutraliser la capacité de réaction des Etats-Unis. Les « pirates » qui participaient à l'exercice étaient en fait des fonctionnaires américains, qui n'avaient reçu aucun renseignement préalable et qui avaient acheté leurs ordinateurs portables dans un magasin d'informatique local.

Les pirates ont démontré qu'ils pouvaient facilement accéder aux systèmes de commande des réseaux d'électricité de toutes les grandes villes américaines, Los Angeles, Chicago, Washington, New York, dont dépendait la capacité de déploiement des forces des Etats-Unis. Qui plus est, ils ont réussi à pénétrer dans le système téléphonique de police secours (le numéro 911) et auraient facilement pu saboter ces deux systèmes.

Ils se sont ensuite attaqués au dispositif de commande et de contrôle du Pentagone. En l'espace de quelques jours, ils ont interrogé environ quarante mille réseaux et ont obtenu l'accès de base à trente six d'entre eux. Ils sont parvenus à pénétrer profondément dans la structure de commande et de contrôle et, s'ils l'avaient voulu, ils auraient pu en perturber le fonctionnement.

Ce que cet exercice a démontré, c'est que trente cinq personnes possédant des informations accessibles à tout un chacun et des moyens techniques disponibles dans le monde entier auraient véritablement pu empêcher les Etats-Unis de réagir à la crise.

C'est là une démonstration remarquable de la puissance redoutable de l'arme informatique. Ce pouvoir a contraint les Etats-Unis à investir des sommes considérables pour se doter de capacités offensives efficaces dans les secteurs où l'on peut livrer bataille autrement que par des moyens classiques.

Pour peu qu'on en ait la capacité, on peut faire la guerre, non pas en déployant des troupes ordinaires sur un champ de bataille, ce qui peut causer des milliers de morts, ni même en tirant des missiles classiques, mais en lançant dans le cyberspace des bits et des octets capables de détruire un agresseur potentiel avant même que les soldats ne s'affrontent sur le terrain.

Dans ce genre d'attaque, il s'agit, par exemple, d'éteindre toutes les lumières d'une grande ville, de fausser les marchés boursiers, ou d'interrompre les flux d'information dans un pays étranger pour y substituer ses propres informations, ce qui permet de lancer des opérations psychologiques très efficaces contre un ennemi potentiel.

Pour bénignes qu'elles puissent paraître, ces interventions peuvent faire autant de victimes qu'une intense campagne de bombardement.

C'est ainsi qu'une étude effectuée par l'Armée de l'air américaine sur les conséquences de la mise hors service du réseau électrique du sud ouest des Etats-Unis a démontré que vingt mille personnes y auraient péri. De telles conséquences auraient un effet catastrophique sur le moral du pays et il se présente donc de nouveaux défis très intéressants sur la manière d'y répondre.

Lors de la récente crise avec l'Irak, il y a quelques mois, alors que nous nous préparions à une éventuelle intervention armée, des tentatives d'intrusion dans le réseau logistique des Etats-Unis ont été détectées. On a fini par trouver que ces tentatives avaient pour origine un immeuble d'Abou Dhabi, et on a immédiatement soupçonné que c'était Saddam Hussein qui lançait une guerre de l'information contre les Etats-Unis afin de prévenir une intervention. Des Américains ont été envoyés sur place pour parer à la menace et, ayant atteint l'immeuble concerné, ils y ont découvert un routeur (point de transfert) d'Internet et ont constaté qu'en fait, cette « attaque » provenait d'adolescents aux Etats-Unis.

C'est là une parfaite illustration des périls et des potentialités de la guerre de l'information. Nous pouvons lancer une attaque, et faire en sorte qu'elle semble provenir d'un lieu très éloigné de son point d'origine réel. Inversement, lorsqu'une attaque est lancée contre nous, il est extrêmement difficile d'en découvrir la source. Même si on la découvre, il est très difficile ensuite de lancer une attaque. Qui doit on attaquer et pourquoi? Quelles seront les réactions du public, quel sera son appui, si les mesures prises font des milliers de morts? Comment persuader les gens que c'était la meilleure option possible? Il n'y aura pas d'enfants morts dans les rues à présenter comme preuves du bien fondé de l'intervention, pas d'homme posté l'arme au poing au coin d'une rue. Le public n'a pas l'habitude de ce genre d'événements et cela présente de réelles difficultés.

Ces questions et les possibilités qu'elles offrent se révèlent très attrayantes pour pratiquement tous les pays dotés de capacités d'intervention dans le domaine de l'information. Pour l'Etat nation, la guerre de l'information a un potentiel attrayant, mais elle est également porteuse de lourdes menaces, parce que cette guerre ne se situe pas au niveau des pays, mais des moyens dont disposent certains particuliers.

La guerre de l'information est, à mon avis, en train de changer fondamentalement la dynamique qui existait depuis très longtemps et qui contribuait à maintenir l'équilibre entre les Etats, à savoir que ce sont les gouvernements qui décident du rythme du changement et qui sont, en général, les principaux agents du changement.

Lorsqu'un nouveau système d'armement est mis au point, il faut un certain temps avant qu'il passe du pays qui l'a créé à un pays qui n'a pas la capacité de le produire: le cycle est d'environ vingt ans. Or, de nos jours, l'ordinateur le plus récent provient de Compaq, les logiciels de Microsoft, et ces outils sont disponibles chez CompUSA (chaîne de magasins d'informatique des Etats-Unis). Le gouvernement l'achètera peut être d'ici deux ou trois ans, mais ce n'est guère probable. En revanche, je puis, moi, me rendre au magasin d'informatique, chèque en main, et m'acheter le matériel. Dans la guerre de l'information, ce matériel est mon arme.

J'ai le pouvoir, les moyens, assis chez moi, muni de mon ordinateur et de mon modem, du moment que je sais comment m'y prendre, de faire la guerre. La situation est radicalement différente de tout ce que nous avons pu connaître par le passé.

Il est particulièrement intéressant, je trouve, au cours de la révolution de l'information à laquelle nous assistons et nous n'en sommes qu'au tout début, de voir les nouvelles alliances qui se développent. J'ai parlé récemment à un ami qui avait organisé une conférence en ligne pour les montagnards, les habitants des montagnes du monde entier, des Alpes ou de l'Oural ou des Rocheuses. Ces montagnards, qui communiquaient entre eux pour la première fois, ont donc participé à une conférence en ligne de deux jours. Ils se sont aperçus qu'ils avaient beaucoup de choses en commun: tous détestent les habitants des vallées, tous se méfient de l'autorité publique, et tous s'intéressent passionnément à l'environnement.

Voilà donc un exemple d'une nouvelle communauté dont les membres ont plus en commun les uns avec les autres qu'ils n'en ont, par exemple, avec leurs compatriotes. Ces groupes, que ce soient les cinquante deux groupements terroristes qui ont actuellement des sites sur le Web, des associations écologistes ou des marginalisés, ont tous à présent la possibilité de se parler, de partager leurs connaissances et d'exprimer leurs frustrations. Il est fascinant de voir l'unité, ou la capacité d'unité, qui existe parmi ces groupes et qui n'existait jamais auparavant.

Bien que nous ne puissions pas éliminer le risque de guerre, nous avons la capacité offensive de faire la

guerre par d'autres moyens et certainement de modifier l'escalade qui mène aux conflits traditionnels. Et ceci présente de réels défis. Tout d'abord, le gouvernement doit comprendre ce qu'une guerre signifie. Nous sommes restés cantonnés dans l'environnement de la guerre froide. Si vous demandez à l'armée de l'air, ou à la marine, ou aux autres entités qui développent actuellement ces nouvelles capacités : « Dans quelles circonstances êtes vous autorisées à en faire usage ? », elles répondent : « Eh bien, nous avons posé cette question au ministère de la justice il y a quelques années, et nous attendons toujours la réponse. »

Or la question est importante. On voudrait employer ces armes juste avant de partir en guerre, de manière à éviter de déclencher une guerre classique. Et pourtant il s'agit d'armes extrêmement agressives et puissantes. Il se posera donc un immense défi au gouvernement et, en fait, c'est déjà le cas : comment se maintenir à niveau alors que tout l'environnement évolue à un rythme aussi rapide ?

Nous devons également, de manière défensive, prendre en compte une différente forme de menace. Traditionnellement, les militaires se considèrent comme des soldats qui montent aux premières lignes, se battent, se font blesser ou tuer, ou ressortent indemnes ; soit ils réussissent, soit ils échouent. Mais dans ce nouvel environnement, nous sommes tous au front. La question est maintenant de savoir comment nous nous défendons, comment nous nous protégeons, et comment nous sommes protégés par le gouvernement ou par le secteur privé. Nous faisons partie de ce processus. Cela constitue un environnement très différent.

Le problème informatique de l'an 2000 le fameux « bogue de l'an 2000 » est une excellente illustration de cette situation. C'est en fait une question sociale, au même titre que la guerre de l'information. Cette guerre peut consister à couper l'alimentation en eau et en électricité, à paralyser les usines de traitement des eaux usées, à bloquer les GAB (guichets automatiques bancaires), bref à détruire les dispositifs de soutien de la vie courante.

Le problème de l'an 2000 et la manière de l'aborder vont démontrer toute l'étendue de l'interdépendance de l'infrastructure essentielle. Personne n'a encore pleinement compris à quel point tout ce que nous faisons est lié. Si une pièce du puzzle est défectueuse, le reste du puzzle se fragmente. Ce n'est pas simplement une question nationale, mais une question internationale.

Nous devons donc, tout en relevant les défis de la guerre de l'information, prendre en compte simultanément les défis posés aux gouvernements. Qu'est ce que cela signifie dans ce nouvel environnement ? Nous devons notamment faire face au danger que court l'infrastructure de base : comment pourrons nous la défendre de manière efficace ?

C'est ici que le secteur privé jouera un rôle vital, parce que c'est lui qui engendre les changements auxquels nous assistons autour de nous. Le gouvernement, pour sa part, doit démontrer sa pertinence et exercer une certaine autorité qui, à mon avis, lui fait actuellement défaut.

Le secteur privé peut s'attaquer à beaucoup de ces dossiers, afin de se défendre et de nous défendre aussi. Si nous ne reconnaissons pas ce fait, je crains que nous nous exposions à de graves conséquences, à commencer par le bogue de l'an 2000. Nous tomberons victimes de nouveaux agresseurs extérieurs, qui auront un pouvoir dont nous n'avons aucune idée. Et lorsque nous aurons compris, il sera trop tard.

Ce que je recommanderais, c'est de sensibiliser les gens à ces questions et d'encourager non seulement une prise de conscience du public, mais également des mesures plus actives de la part de ceux qui peuvent diffuser l'information, de façon à mettre en place des dispositifs de défense contre un environnement qui promet d'être extrêmement périlleux au cours du siècle prochain. ●

FICHE DOCUMENTAIRE : LA PROTECTION DE L'INFRASTRUCTURE DE BASE AUX ETATS-UNIS

(Décret présidentiel 63)

Document rendu public le 22 mai 1998 par la Maison-Blanche

Le décret présidentiel approfondit les recommandations de la Commission présidentielle sur la protection de l'infrastructure de base. Dans son rapport rendu public en octobre 1997, la Commission préconise la mise en œuvre d'une action nationale visant à assurer la sûreté de diverses composantes de l'infrastructure des Etats-Unis dont la vulnérabilité et l'interdépendance vont croissant. Les secteurs concernés regroupent notamment les télécommunications, les établissements bancaires et financiers, l'énergie, les transports et les services publics essentiels.

Le décret présidentiel 63 est l'aboutissement d'efforts intenses qui ont été déployés à l'échelon interministériel dans le souci d'évaluer ces recommandations et d'arrêter un cadre pratique et novateur relatif à la protection de l'infrastructure de base. En voici le détail :

– Il propose de mettre en place, d'ici à l'an 2003, des réseaux d'information fiables, interconnectés et capables de garantir la sécurité des transmissions, et il se fixe l'objectif de la sécurisation nettement accrue des systèmes du secteur public d'ici à l'an 2000. A cette double fin, il prévoit :

- a) L'établissement immédiat d'un centre national qui aurait pour mission de donner l'alerte en cas d'attaque et de prendre les mesures voulues pour y riposter ;
- b) La création, d'ici à l'an 2003, de la capacité nécessaire à la protection de l'infrastructure de base contre les actes de sabotage.

– Il s'attaque à la question de la vulnérabilité de l'infrastructure électronique et matérielle du gouvernement fédéral en donnant pour consigne à tous les ministères et à tous les organes publics de trouver des moyens d'atténuer les risques que pourraient entraîner de nouveaux dangers.

– Il donne l'ordre au gouvernement fédéral de servir de modèle au reste du pays quant aux moyens de protéger l'infrastructure.

– Il recherche la participation volontaire de l'industrie privée, notamment sous forme de partenariats avec le secteur public, pour atteindre l'objectif commun de la protection des systèmes essentiels.

– Il protège le principe de la confidentialité et cherche à tirer parti des forces du marché. L'objectif doit être de renforcer et de protéger le pouvoir économique du pays, et non pas de l'étouffer.

– Il recherche la pleine participation du Congrès et compte sur l'initiative des parlementaires.

Le décret présidentiel 63 annonce la création d'une nouvelle structure dont la nécessité s'explique par l'importance des enjeux :

– Elle concerne notamment la création d'un poste de coordonnateur national, lequel s'occupera non seulement de l'infrastructure de base, mais aussi du terrorisme à l'étranger et des menaces de destruction massive sur le plan intérieur (y compris en cas d'utilisation d'armes biologiques), parce que les attaques dont les Etats-Unis pourraient faire l'objet peuvent très bien recouper plusieurs domaines d'intervention.

– Elle prévoit l'établissement d'un Centre de protection de l'infrastructure nationale (NIPC, « National Infrastructure Protection Center ») au sein du Bureau fédéral d'enquête (FBI). Le NIPC regroupera des représentants du FBI, du ministère de la défense, des services secrets, du ministère de l'énergie, du ministère des transports, des milieux du renseignement et du secteur privé dans un effort sans

précédent d'échange d'information entre ces organes, et ce en collaboration avec le secteur privé. De surcroît, le NIPC fournira le gros des efforts pour ce qui est de faciliter et de coordonner la réponse du gouvernement fédéral en cas de circonstances critiques, d'atténuer les conséquences d'attaques éventuelles, d'enquêter sur les dangers probables et de surveiller les travaux de remise en état.

- Elle encourage le secteur privé à créer un Centre d'échange et d'analyse des informations (ISAC, « Information Sharing and Analysis Center ») en coopération avec le gouvernement fédéral.
- Elle comprendra aussi un Conseil de sûreté de l'infrastructure nationale (« National Infrastructure Assurance Council ») dont les membres seront recrutés parmi les personnalités dirigeantes du secteur privé et les responsables à l'échelon local et des Etats. Ce conseil aura pour tâche de guider les pouvoirs publics en matière de formulation d'un plan national.

– l'Office de sûreté de l'infrastructure de base (« Critical Infrastructure Assurance Office ») apportera son concours au coordonnateur national qui aura pour tâche de formuler un plan national en œuvrant de concert avec des organismes publics et le secteur privé. Cet office participera également à la coordination d'un programme national d'éducation et de sensibilisation ainsi qu'à la conduite des affaires parlementaires et relatives aux relations publiques.

Pour de plus amples renseignements sur ce décret, veuillez contacter l'Office de sûreté de l'infrastructure de base au 703 696 9395 et demander un exemplaire du Livre blanc sur la protection de l'infrastructure de base (« White Paper on Critical Infrastructure Protection »).



ARTICLE RECENTS (*en anglais*)

Articles relatifs à la guerre informatique

Bennett, Robert, et al. THE Y2K CRISIS: A GLOBAL TICKING TIME BOMB? (The Washington Quarterly, vol. 21, no. 4, Autumn 1998, pp. 147-166)
 Management consultants, financial planners, and experts in year 2000 conversion issues warn, in five essays, that the Y2K computer problem deserves to be taken seriously — and soon, before it is too late. Senator Bennett, who chairs a Senate Special Committee on the Y2K problem, says the “biggest challenge” is “to get people thinking... across the individual lines of our own organizations, indeed across the individual lines of our own country’s borders.” And “we must...recognize that this is not an IT (information technology) problem” but rather “a management challenge” that must be addressed immediately at the highest levels, he says.

Bowers, Stephen R. INFORMATION WARFARE: THE COMPUTER REVOLUTION IS ALTERING HOW FUTURE WARS WILL BE CONDUCTED (Armed Forces Journal International, August 1998, pp. 38-39)
 Contending that access to information today is just as crucial as possession of petroleum and ammunition, Bowers discusses the threat posed by “almost invisible computer assailants” to a nation’s power grids, transportation networks, financial systems, and telephone exchanges. He says recent U.S. military exercises have involved actions that elevate IW (information warfare) from a tactical to a strategic level. IW involves a new kind of battlefield but with the potential for equally as many casualties, he says.

Gompert, David C. NATIONAL SECURITY IN THE INFORMATION AGE (Naval War College Review, vol. 51, no. 4, sequence 364, Autumn 1998, pp. 22-41)
 Gompert, director of the National Defense Research Institute at RAND, argues that the changes brought about by the information revolution, though not without drawbacks, have greatly benefited the United States. The information revolution has extended economic and political freedom, Gompert states, expanding the world’s “democratic core.” It has brought about significant changes in the conduct of warfare, giving the United States, with its lead in information technology, a great advantage: “Roughly stated, information technology can help those who master it to win large wars at long distances with small forces,”

says Gompert. He cites a concern that rogue states “are likely to turn to asymmetric strategies, for instance, weapons of mass destruction, terrorism, and information warfare (IW) attacks against the United States and its partners.”

Henry, Ryan; Peartree, C. Edward. MILITARY THEORY AND INFORMATION WARFARE (Parameters, vol. 28, no. 3, Autumn 1998, pp. 121-135)
 The authors examine the limited influence that technologies have had on warfare and cite as an example the airplane, which, though adding an unprecedented technological breakthrough to the battle space, repeatedly has been shown to be insufficient in and of itself to transform war. Old weapons do not necessarily go out of style — “new tools are just added to the box,” the authors say. Underscoring the importance of grasping “the functional significance of technological innovations,” they contend “it is equally important that risks and vulnerabilities — the stuff of strategy — remain foremost in assessing their political and military implications. The most durable military theory focuses less on the latest technology and more on the infinite complexity of the user.”

Selden, Zachary. MICROCHIPS AND THE MILLENNIUM: THE NATIONAL SECURITY IMPLICATIONS OF THE YEAR 2000 PROBLEM (National Security Studies Quarterly, vol. 4, issue 3, Summer 1998, pp. 71-77)
 Selden predicts that most computer software associated with the year 2000 problem will be fixed or discarded and that most of the problematic embedded computer chips will be replaced by January 1, 2000. What remains could cause unpredictable failures or sow confusion sufficient to allow states or terrorists to conduct covert disruptions or intrusions, he says. International actors may seek “to take advantage of a distracted United States” at the turn of the millennium, the author warns, and some current regional flash points might erupt “into a spiral of conflict because of failed systems.” From a national security perspective the problem “is the perception that Y2K presents a window of vulnerability,” the author says.

The annotations above are part of a more comprehensive Article Alert offered on the home page of the U.S. Information Service: “<http://www.usia.gov/admin/001/wwwhapub.html>”. ◎

BIBLIOGRAPHIE (*en anglais*)

Publications permettant d'explorer d'autres points de vue sur la protection des systèmes informatiques

Adams, James. THE NEXT WORLD WAR: COMPUTERS ARE THE WEAPONS AND THE FRONT LINE IS EVERYWHERE. New York: Simon & Schuster, 1998. 366p.

Arquilla, John; Ronfeldt, David F. (Editors). IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE. Santa Monica, CA: Rand, 1997. 501p.

Barnett, Roger W. INFORMATION OPERATIONS, DETERRENCE, AND THE USE OF FORCE (Naval War College Review, vol. 51, no. 2, Spring 1998, pp. 7-19)

Browne, J.P.R.; Thurbon, M.T. ELECTRONIC WARFARE, Vol. 4 of Brassey's Air Power: Aircraft Weapons Systems and Technology Series. Washington: Brassey's, 1998. 341p.

Cillufo, Frank J.; Tomarchio, Thomas. RESPONDING TO NEW TERRORIST THREATS (Orbis, vol. 42, no. 3, Summer 1998, pp. 439-452)

Clinton, William J. COMMENCEMENT ADDRESS AT THE UNITED STATES NAVAL ACADEMY IN ANNAPOLIS, MARYLAND (Weekly Compilation of Presidential Documents, vol. 34, no. 21, May 22, 1998, pp. 944-948)

Copley, Gregory R. RE-DEFINING PSYCHOLOGICAL STRATEGY IN THE AGE OF INFORMATION WARFARE (Defense & Foreign Affairs Strategic Policy, vol. 26, no. 6, June 1998, pp. 5-8)

Gunther, Christopher. YOU CALL THIS A REVOLUTION? (Foreign Service Journal, vol. 75, no. 9, September 1998, pp. 18-23)

Henry, Ryan; Peartree, C. Edward (Editors). INFORMATION REVOLUTION AND INTERNATIONAL SECURITY (Significant Issues Series, vol. 20, no. 1). Washington: Center for Strategic & International Studies, 1998. 216p.

Libicki, Martin C. INFORMATION WAR, INFORMATION PEACE (Journal of International Affairs, vol. 51, no. 2, Spring 1998, pp. 411-428)

Molander, Roger C.; Riddile, Andrew S.; Wilson, Peter A. STRATEGIC INFORMATION WARFARE: A NEW FACE OF WAR. Santa Monica, CA: Rand, 1996. 90p.

Petersen, John L.; Wheatley, Margaret; Kellner-Rogers, Myron. THE YEAR 2000: SOCIAL CHAOS OR SOCIAL TRANSFORMATION? (The Washington Quarterly, vol. 21, no. 4, Autumn 1998, pp. 129-146)

Pfaltzgraff, Robert L.; Schultz, Richard H. (Editors). WAR IN THE INFORMATION AGE: NEW CHALLENGE FOR U.S. SECURITY POLICY. Washington: Brassey's, 1997. 320p.

Rathmell, Andrew. INFORMATION WARFARE: USA TACKLES CYBERTHREAT (Jane's Intelligence Review Pointer, vol. 5, no. 9, September 1, 1998, p. 14)

Ryan, Stephen M. SHOULD U.S. PLEDGE NOT TO MAKE FIRST CYBERSTRIKE? (Government Computer News, vol. 17, no. 24, August 3, 1998, p. 32)

Sanz, Timothy L. INFORMATION-AGE WARFARE: A WORKING BIBLIOGRAPHY (Military Review, vol. 78, no. 2, March-April 1998, pp. 83-90)

U.S. Senate, Select Committee on Intelligence. CURRENT AND PROJECTED NATIONAL SECURITY THREATS TO THE UNITED STATES. Washington: Government Printing Office, 1998. 177p.

Verton, Daniel. DOD PREPS OFFICE FOR CYBERDEFENSE (Federal Computer Week, vol. 12, no. 23, July 13, 1998, pp. 1-2) ●

SITES INTERNET (*en anglais*)

Principaux sites se rapportant à la protection des systèmes informatiques

Veillez noter que l'USIA n'est nullement responsable du contenu des sites indiqués ci-après

Air Force Information Warfare Center
<http://www.afiw.c.aia.af.mil/>

Center for High Assurance Computer Systems of the
Naval Research Laboratory
<http://www.itd.nrl.navy.mil/ITD/5540/main.html>

Computer Security Technology Center, Lawrence Livermore
National Laboratory, U.S. Department of Energy
<http://ciac.llnl.gov/cstc/>

Critical Infrastructure Assurance Office
<http://www.ciao.gov/>

Cyberspace Policy Institute at George Washington University
<http://www.seas.gwu.edu/seas/institutes/cpi/>

Defense Information Infrastructure
<http://spider.osfl.disa.mil/dii/>

Defense Policy on the Year 2000 Computer Conversion Issue
<http://www.defenselink.mil/issues/y2k.html>

Glossary of Information Warfare Terms
<http://www.psycom.net/iwar.2.html>

IBM Corporation: Secure Way
<http://www.ibm.com/Security/>

Information Systems Security Association
<http://www.issa-intl.org/>

Information Warfare Academic Group,
Naval Postgraduate School
<http://web.nps.navy.mil/~iwag/>

Information Warfare and Information Security on the Web
<http://www.fas.org/irp/wwwinfo.html>

Information Warfare: Glossary
<http://www.informatik.umu.se/%7Erwhit/IWGlossary.html>

Information Warfare Research Center
<http://www.terrorism.com/infowar/documents.html>

InfoWar.Com
<http://www.infowar.com/main.html>

Infrastructure Defense, Inc.
<http://206.132.10.154/idmarketsite/>

Microsoft Corporation (Key Initiatives)
<http://www.microsoft.com/>

National Colloquium for Information Systems Security
<http://www.infosec.jmu.edu/ncisse/>

National Infrastructure Protection Center of the Federal
Bureau of Investigation
<http://www.fbi.gov/nipc/home.htm>

National Institute of Standards and Technology (NIST)
<http://csrc.nist.gov/>

National Security Agency
<http://www.nsa.gov:8080/>

President's Council on Year 2000 Conversion
<http://www.Y2K.gov/java/index.htm>

School of Information Warfare and Strategy, National
Defense University
<http://www.ndu.edu/inss/act/iwscvr.html>

Technology News: Governments Beat Terrorists To Net
Weapons
<http://www.techweb.com:80/wire/story/TWB19980922S0018>

U.S. Senate, Committee on the Judiciary, Subcommittee
on Technology, Terrorism, and Government Information
<http://www.senate.gov/~judiciary/terrtest.htm>


Year 2000 Conversion: U.S. Information Agency
<http://www.usia.gov/topical/global/y2k/>

LES OBJECTIFS DE POLITIQUE ETRANGERE DES ETATS-UNIS

VOLUME 3

REVUE ELECTRONIQUE DE L'AGENCE D'INFORMATION DES ETATS-UNIS

NUMERO 4



*Cybermenace:
la protection
des réseaux
informatiques
des Etats-Unis*

Novembre 1998