DES RISQUES AUX MENACES : LES NOUVELLES VULNÉRABILITÉS DE LA SOCIÉTÉ DE L'INFORMATION

par

Anne AZAM-PRADEILLES

Chargée de mission auprès du Directeur de la Défense et de la Sécurité civile [1]

Adjointe au chef de la Mission de défense et continuité nationale

« By decision of the government the Ministry of Defence set up on May 26, 1977, the Committee on the Vulnerability of Computer Systems (SARK) to investigate the vulnerability of the computerized society and to propose measures to reduce it

The task of the Committe is not confined to counteracting risks in connection with military preparedned and war but is also to consider other situations involving threat and pressure.

SARK divides the vulnerability factors in two main categories, external and internal. The first is concerned with different attacks from without, e.g. acts of war and terrorist actions. The second comprises such factors as are more or less built into the actual use of computers, e.g. the concentration of computer operations, the dependence on competent staff and on assistance from abroad.
SARK's study must be made from the perspective of total defence. »

Preliminary Report by a Swedish Governement Committee, Ministry of Defence, Stockholm, 1978 [2].

Ainsi, il y a plus de vingt ans, la vulnérabilité de la société de l'information, inhérente à sa nature même, était déjà affirmée. Mais cette prise de conscience s'est longtemps trouvée reléguée au second plan par l'optimisme général suscitée par l'extraordinaire puissance conférée par les systèmes d'information.

Avec la disparition de l'équilibre étatique de la terreur après la chute du mur de Berlin, l'émergence de nouveaux risques et de nouvelles menaces, plus diffus, complexes et immatériels, portant non

1 Haut fonctionnaire de défense du ministère de l'Intérieur

2 Traduction : « *Par décision du gouvernement, le ministre de la Défense [de la Suède] a instauré le 26 mai 1977 le Comité sur la Vulnérabilité des Systèmes d'Information (CVSI) pour effectuer des recherches sur la vulnérabilité de la société informatisée et pour proposer des mesures afin de la réduire.*
La mission du Comité ne se limite pas à riposter aux risques inhérents à la veille opérationnelle militaire et à la guerre mais comporte aussi d'autres situations porteuses de menaces et de pressions.
Le CVSI divise les facteurs de vulnérabilité en deux catégories, l'une externe, l'autre interne.
La première a trait aux différentes attaques en provenance de l'extérieur, comme par exemple des actes de guerre ou des actions terroristes.
La seconde comprend des facteurs qui sont plus ou moins partie intégrante de l'utilisation concrète des ordinateurs, comme la concentration des opérations informatiques, la dépendance par rapport à un personnel compétent et par rapport à une assistance en provenance de l'étranger.
L'étude du CVSI s'inscrit dans une perpective de défense globale. »
Rapport préliminaire d'un comité du gouvernement suédois, Stockholm, 1978, extrait de *This Quiet Revolution*, Y. Leray, A. Pradeilles, N. Vigouroux-Frey, Paris : A. Colin-Longman, 1980, pp. 160-161.

seulement sur des secteurs nouveaux, économiques, scientifiques, technologiques, voire culturels, mais encore et surtout selon des modalités nouvelles, terrorisme, mafias, grand banditisme, cybercrime etc., plus difficiles à identifier et à combattre, les systèmes d'information, instruments de puissance et de pouvoir, sont devenus, par leur imbrication au sein de l'infosphère, réseau mondial sans frontière et sans loi, une des nouvelles vulnérabilités majeures de la société moderne à l'aube du troisième millénaire.

Après avoir retracé les étapes qui ont marqué l'avènement de la société de l'information et montré comment on est aujourd'hui passé des risques aux menaces, nous analyserons les formes de la prise de conscience actuelle de ses vulnérabilités, notamment en termes de réponse juridique.

I. DE ENIAC A I-MAC OU DE LA CYBERNETIQUE DE SCIENCE-FICTION AU TERMINAL INTERNET EN SUPERMARCHE

1.1. A l'aube des ordinateurs : les premiers efforts des scientifiques pour automatiser les calculs

Après la Pascaline de Blaise Pascal en 1642, la machine trigonométrique et astronomique de Leibniz en 1694 et les premiers métiers de Jacquard en 1804, c'est en 1822 que le mathématicien anglais Charles Babbage conçut le véritable ancêtre de nos ordinateurs, « *the Difference Engine* ». Mais la fille du grand poète Byron, Ada, considérée comme la première informaticienne, ne put tester ses programmes sur la seconde machine de Babbage, « *the Analytical Engine* », jamais réellement opérationnelle. Il fallut attendre près d'un siècle : Mark I fut offert en 1944 à l'Université de Standford par International Business Machines, entreprise spécialisée dans les tabulateurs électriques depuis la fin du dix-neuvième siècle et encore aujourd'hui sans doute la marque la plus célèbre d'ordinateurs, IBM.

La seconde guerre mondiale a indéniablement accéléré la mutation vers le premier ordinateur électronique en 1946, ENIAC, *Electronic Numerical Integrator and Calculator*, développé pour l'armée américaine à l'Université de Pennsylvanie par Eckert et Mauchly.

Parallèlement, Von Neumann développait les concepts de mémoire et de traitement des données à partir de programmes stockés dans la mémoire de la machine. L'ordinateur moderne était né. Ensuite, matériel et logiciel se sont mutuellement fait progresser, en taille, en complexité, en performance et en coût.

1.2. De la naissance de la société de l'information aux premières perceptions de ses dangers

Tout processus connaît un cycle de vie, depuis sa naissance ou apparition jusqu'à sa mort ou disparition.

On peut considérer que la société de l'information est née avec ENIAC, le premier ordinateur "moderne" à la fin de la deuxième guerre mondiale. Le progrès était alors synonyme d'ouverture, de vitesse, d'accessibilité. L'informatique et les systèmes d'information étaient l'apanage d'un cercle très fermé de scientifiques, souvent issus du monde militaire ou de celui de la recherche, mondes d'ailleurs encore très imbriqués.

Les risques étaient essentiellement techniques, générés par les limites et insuffisances des machines et des programmes. Les « *bugs* » étaient alors de vrais insectes venus s'enchevêtrer dans les écheveaux compliqués des kilomètres de cablages et de lampes. **Les menaces** étaient principalement militaires, éventuellement liées au nucléaire, et, dans le domaine économique, surtout orientées contre les industries liées à la défense militaire et à la conquête de l'espace.

Les performances des ordinateurs permettaient - ou limitaient - les réussites : avec le premier Spoutnik en 1957 et le premier vol de Youri Gagarine autour de la Terre en 1961, l'URSS prenait un avantage que les Américains ont mis quelques années à rattraper.

La cybernétique faisait rêver, mais, derrière HAL, l'ordinateur pensant de « 2001, l'odyssée de l'espace », se cachait IBM - décalé d'une lettre vers la droite. Et, dans

1984, George Orwell présentait dès 1948 les dangers de « *big brother* » - un temps rebaptisé « *blue brother* » en référence au même géant de l'informatique.

Les progrès techniques de l'informatique spatiale, notamment les premiers pas américains sur la Lune en 1969, et le succès de l'informatisation du monde de l'entreprise, en particulier avec les gros systèmes comme le légendaire IBM 360 ou les machines d'ICL et de BULL, changèrent considérablement les données du problème.

Même si la comparaison peut sembler hardie, on ne peut s'empêcher de constater le parallèle saisissant qui existe entre la théorie de Darwin sur l'évolution des espèces et les évolutions technologiques et méthodologiques qui ont structuré le monde de l'informatique et des ordinateurs au cours des quarante dernières années, qui peuvent se diviser en quatre grandes étapes.

1.3. Des gros systèmes professionnels sécurisés à la libération des ordinateurs individuels

Les années 60-70 consacrent l'avènement des gros systèmes et la culture du secret, outil de pouvoir.

Une *informatique centralisée*, gérée par des services informatiques spécialisés et sécurisés, avec des salles machines exigeant des contraintes matérielles (climatisation en particulier) et des programmes à la syntaxe encore très proche du code machine (assembleur, FORTRAN [3], COBOL [4]) imposant une formation technologique importante des personnels, limitent encore les risques et les menaces pesant sur l'information. Les informaticiens sont imprégnés d'**une culture du secret**.

L'information étant une composante forte du pouvoir, ils sont peu enclins à la partager. Tels des grands prêtres, ils inspirent admiration et parfois crainte. Les centres de calcul sont gardés comme des Fort Knox et sont au cœur des romans d'espionnage.

En libérant l'informatique, les premiers ordinateurs individuels deviennent des instruments de puissance ... et de vulnérabilité.

Les APPLE de Steve Jobs, conçus selon la légende dans son garage à la fin des années 70, puis l'introduction des PC (*Personal Computers* [5]) de la firme IBM au tout début des années 80 changent radicalement l'approche de l'informatique et constituent une sorte de révolution culturelle : d'une informatique centralisée, "jacobine", garante d'ordre, d'organisation et de sécurité, on passe à une explosion d'initiatives et **une diffusion d'informations tous azimuts**, à un éparpillement, parfois incohérent voire contre productif, qui gagne même le monde de l'entreprise.

L'imagination a pris le pouvoir et les concepts d'informatique domestique et d'informatique ludique apparaissent. La puissance croissante des capacités machine - avec le déblocage des 640 K [6] de mémoire vive, l'invention des disquettes souples puis rigides, des disques durs - rend possible l'élaboration de langages informatiques de plus en plus conviviaux, avec de plus en plus de couches utilisateurs. L'informatique devient accessible à tous. On est ainsi passé des systèmes d'exploitations de type CP/M ou DOS [7], encore réservés à l'initié, au mode iconique du Macintosh, qui ouvrira la voie, quelques années plus tard, aux fenêtres de WINDOWS. Les anglo-saxons inventent le concept de « *userfriendliness* » : le PC devient l'ami. C'est l'avènement de l'individualisme et de la liberté.

3 FORTRAN, acronyme de *Formula Translation*, « traducteur de formules », langage d'inspiration très mathématique destiné aux applications scientifiques, créé en 1955 et encore utilisé parfois dans sa version FORTRAN IV.

4 COBOL, acronyme de *Common Business Oriented Language*, crée en 1959 par un comité réuni au Pentagone afin de concevoir un langage commun pour le traitement des données du monde de la gestion, du commerce, des administrations et des affaires. De nombreuses entreprises vivent encore sur des montagnes de COBOL et c'est grâce à un ingénieux économe de mémoire que le monde est secoué par le « bug de l'an 2000 »...

5 PC : ordinateurs personnels.

6 K : kilos octets. Aujourd'hui on compte plutôt en Mo, méga-octets et Go, giga-octets. On est passé de mille au million et au milliard.

7 CP/M : *Computer programming / memory ;* DOS : *Disk Operating System.*

Mais, si la fiabilité des matériels rend **les risques** accidentels de plus en plus rares, de nouvelles **menaces** apparaissent, ainsi que le nouveau concept de *délinquance informatique* - depuis le vol traditionnel, physique, de matériel et logiciel, en passant par les détériorations physiques et logicielles, la copie frauduleuse, et surtout la production de virus.

Dans le cadre de la guerre froide, *l'arme logicielle* des virus semble avoir été utilisée, avec efficacité, par le bloc soviétique. Mais la foule des amateurs fascinés par l'outil informatique et sa dimension ludique, son ouverture à tous, sa facilité d'accès et d'utilisation ont fait perdre les repères, en particulier dans la jeunesse – véritable pépinière de *hackers* et *crackers* [8], parfois géniaux, parfois rattrapés par la justice ou récupérés par des services spéciaux.

Des premières réactions se font jour dans le monde occidental et au Japon.

Certains pays commencent à prendre conscience de façon aiguë de la fragilisation induite par le fait de confier l'organisation et la défense d'un pays à un système d'information, de dématérialiser les procédures et de les concentrer, enfin de les confier à des experts (cf. le rapport suédois de 1978 sur la vulnérabilité cité en exergue). En France, le Secrétariat général de la défense nationale publie dès le 6 décembre 1976 l'instruction interministérielle n° 1900/SGDN/SSD sur la protection du secret de défense en informatique.

Et pour ce qui est de la protection de la vie privée et des libertés individuelles, la loi « Informatique et Libertés », en 1978, encadre la création des fichiers nominatifs et instaure le droit de regard de la personne fichée.

La relation homme-machine entre dans une phase moins émotionnelle. L'intelligence artificielle perd son aura de science-fiction pour retrouver son statut objectif d'instrument de recherche ou d'outil d'aide à la décision. Les droits démocratiques de l'homme sont réaffirmés face à la machine. L'informatique entre dans l'âge adulte et il y a de la place pour plusieurs informatiques, celle du monde de l'entreprise, celle de l'école, de la recherche et celle du jeu.

1.4. De la rationalisation des réseaux locaux à l'explosion de la toile : une maturité nouvelle mais des menaces plus fortes

Le milieu des années 80 voit se développer une intense réflexion de réappropriation de l'outil informatique par les professionnels et l'entreprise, une prise de conscience de la nécessité de réglementer ces nouvelles activités.

Un grand débat s'instaure, au plan national et international, sur les droits de propriété intellectuelle, mis à mal par les nouveaux supports d'information. La généralisation des photocopieurs dans tous les secteurs d'activité mobilise le monde de l'édition, en lutte contre le « phocopillage ». La généralisation des disquettes - et donc de la copie facile, quasi instantanée d'informations (langages, programmes et données) - ayant provoqué une explosion du *piratage informatique* et un phénomène de copie universel, y compris dans les administrations chargées de la répression des délits et des fraudes ... les éditeurs de logiciels réagissent. En France, à la suite de négociations importantes, une loi précise en 1985 les contours de la propriété intellectuelle des logiciels, ce qui entraîne une baisse des prix de vente et la création des licences multipostes, en particulier pour le monde de l'enseignement et de la recherche, lieu affirmé comme étant celui de l' « Informatique pour tous ».

Dans les entreprises, un gros travail de réorganisation, restructuration, regroupement et rationalisation s'effectue, avec un effort de formation technique et juridique des personnels. La mise en réseau, locaux ou à distance - LANs et WANs [9] - des micro-ordinateurs commence et l'entreprise se tourne vers une *informatique répartie*.

8 Le *hacker* est un pirate, il copie, c'est-à-dire vole, des logiciels ; le *cracker* est un casseur de code, il pénètre dans les systèmes et a donc une grande capacité de nuisance s'il est malveillant.

9 *LAN : Local area network ; WAN : Wide area network.*

Les risques portant sur l'intégrité des données sont de plus en plus étudiés et des solutions trouvées. Aux virus, on oppose des anti-virus et on assiste à une émulation forte des concepteurs des deux types de logiciels. L'ordinateur individuel est naturellement protégé par la barrière physique créée par son isolement - tant qu'on ne lui a pas introduit d'agents extérieurs par l'intermédiaire d'une disquette. Sur un réseau, aux multiples points d'entrée, difficilement contrôlables et sécurisables physiquement, il faut concevoir des barrières logiques, des mots de passe, une cryptologie, des « murs de feu ».

Mais, à cette échelle, la guerre de l'information et donc **les menaces** étaient encore de type classique, quasi-militaires, comme le montre très bien le film « *Wargames* » : le jeune héros pénètre par jeu dans l'ordinateur du Pentagone et y déclenche un engrenage de réactions susceptibles de provoquer une guerre nucléaire avec l'URSS.

Le début des années 90 et la vulgarisation d'Internet [10] marquent une nouvelle étape et même une rupture : en offrant un espace sans foi ni loi [11], la toile constitue un nouvel espace stratégique et l'infosphère est l'enjeu majeur d'aujourd'hui. Internet est la nouvelle frontière, un espace à conquérir, le nouveau champ de bataille d'un type de guerre totalement nouveau.

La nouvelle guerre de l'information se situe à trois niveaux : les individus, les entreprises, les "intérêts fondamentaux de la nation" [12] - chacun ayant des incidences majeures, directes et indirectes sur les deux autres.

La guerre virtuelle, dématérialisée, n'est plus seulement militaire. Un microordinateur couplé à un modem peut faire plus de dégâts qu'un bombardier ou un sous-marin. Mais si cette guerre est "transparente", invisible et méconnue, elle a un coût redoutable. Bien que difficilement évaluables, ses "pertes" sont souvent chiffrées en milliards de francs par an pour la France [13] et ses "morts" et "blessés" se traduisent en autant de chômeurs.

II. UNE NOUVELLE COMBATIVITE : LA REACTION AUX ATTAQUES

2.1. Le modèle américain

En réaction à ces attaques, à partir de 1998, comme l'a annoncé le président Clinton en mai dans un important discours devant la promotion sortante de l'École navale américaine [14], les États-Unis vont consacrer à la sécurisation de leurs systèmes d'information un budget public de 1 milliard de dollars par an jusqu'en 2004 [15]. De plus, parallèlement à l'invasion par le commerce américain d'Internet, réseau non sécurisé, très fragile et donc non fiable, le gouvernement américain a créé un réseau spécial, Intelink, hautement sécurisé, chiffré, fonctionnant sur le DSNET du Pentagone et ne regroupant que les 3 à 4 000 plus hauts responsables habilités "secret" ou "très secret". Ainsi, *une sanctuarisation cybernétique* des principales infrastructures du territoire américain est mise en place, plaçant les autorités du pays hors d'atteinte en cas d'attaque massive sur les réseaux. On notera la terminologie délibérement militaire de ces décisions.

Enfin, les systèmes d'information - outils privilégiés de l'intelligence économique - constituent aujourd'hui à la fois le champ de bataille et l'arme essentiels de la guerre

10 Alors que le réseau (*net*) est crée en décembre 1969, de façon très confidentielle, le site WORLD (monde), première ligne commerciale commutée pour le public, est crée en 1990. Le WWW (*World Wide Web*) est inventé en 1992 par Tim Berners-Lee.

11 Le dernier rapport du Conseil d'Etat sur les réseaux numériques (juin 1998), à la surprise de beaucoup, adopte une position « moderne » de responsabilisation des acteurs, sans proposer d'encadrement législatif ou réglementaire.

12 Les « Intérêts Fondamentaux de la Nation » ont été précisés en 1992 dans le nouveau code pénal (Livre IV, Titre 1er, Art. 410-1) et leur atteinte est passible d'amendes voire d'emprisonnement. En plus des intérêts traditionnels (intégrité du territoire, sécurité etc .), ils incluent l'environnement et *« les élements essentiels du potentiel scientifique et économique* (ainsi que) *le patrimoine culturel* ».

13 En 1996, les pertes dans le secteur informatique ont été évaluées à 13 MrdsF dont 5 pour les pannes et accidents et 8 pour les actes de malveillance.

14 Académie navale d'Annapolis, Maryland, 22 ami 1998.

15 Rapport MARSH de la PCCIP (*President's Commission on Critical Infrastructure Protection*)

économique mondiale, mais aussi culturelle, dans laquelle nous nous débattons, souvent sans même le savoir.

Dans l'infosphère, les risques induits par toutes les menaces nouvelles qui pèsent sur le réseau du fait de sa nature même, totalement ouverte et libre, sont donc venus s'ajouter aux risques traditionnels.

2.2. Les efforts français

La France a très tôt mesuré les enjeux stratégiques de l'informatique.

Sur le modèle de l'indépendance nucléaire, le « Plan calcul » voulu par le Général de Gaulle avait l'ambition d'assurer l'indépendance et la suffisance de la nation en matière de systèmes d'information (moyens matériels, logiciels et même humains). L'exécution du plan ne fut pas à la hauteur des espérances. Si aujourd'hui la France reste un des meilleurs pays dans le domaine de la conception des logiciels et de la formation en informatique, l'industrie nationale des ordinateurs a presque complètement disparu. Et, comme le reste du monde, elle est à la merci des géants américains, MICROSOFT et LOTUS pour tous les logiciels grand public et INTEL pour les microprocesseurs, avec tout ce que cela implique comme dépendance dès qu'il s'agit de sécuriser ou de crypter un système.

Depuis 1976 et l'instruction interministérielle sur la protection du secret de défense en informatique (cf. ci-dessus), la France s'est peu à peu dotée d'un arsenal juridique, plus ou moins contraignant et surtout plus ou moins protecteur dans le monde dérégulé de l'immatériel fugace, volatil et sans frontière (cf. Annexe).

Nous retiendrons quelques étapes importantes de cette prise en compte de la vulnérabilité des systèmes d'information et donc de la société de l'information.

Le 20 juillet 1993, le SGDN a publié une refonte de l'instruction de 1976 : l'instruction générale interministérielle sur la sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées, n° 900/SGDN/SSD/DR et n° 900/DISS/SCSSI/DR.
La nouveauté importante à souligner est l'élargissement de la réponse gouvernementale aux entreprises privées qui font, dans le même temps, l'objet de la recommandation n° 901. Certes une « recommandation » n'est pas une « instruction » et sa force juridique est limitée, mais elle a le mérite d'exister et de servir de signal fort.

L'instruction interministérielle sur la protection du patrimoine scientifique français dans les échanges internationaux, l'IIM 486, du 1er mars 1993, ne consacrait encore qu'une page à la vulnérabilité des systèmes d'information. Elle est en cours d'actualisation pour intégrer les évolutions déjà importantes intervenues depuis cinq ans dans ce domaine technologique très sensible et omniprésent dans pratiquement tous les secteurs d'activité.

En 1994, la Délégation Interministérielle pour la Sécurité des Systèmes d'Information [16], dans un rapport au Premier ministre sur les attaques informatiques, a apporté une contribution essentielle au débat en faisant le point et en procédant à une nécessaire synthèse. Elle a ainsi identifié :

- six types de menaces intentionnelles : stratégique, idéologique, terroriste, cupide, ludique et vengeur, ces caractéristiques étant souvent combinées entre elles ;

- sept catégories de menace : l'espionnage, la perturbation, le vol, la fraude physique, le chantage, le sabotage et les accès illégitimes.

- les nombreuses motivations de ces actes : espionnage, appât du gain, fraude, vol, piratage, défi intellectuel, vengeance, chantage, extorsion de fonds etc. sans oublier curiosité, ennui, paresse, ignorance, incompétence, inattention, etc.

- quatre profils d'attaquants : les pirates (*hackers* et *crackers*) [17], les fraudeurs

16 DISSI/SCSSI N° 650, Issy-Les-Moulineaux 28 mars 1994.
17 *Hacker* : pirate par jeu ou par défi; *cracker* : pirate plus dangereux, qui cherche à nuire (cf. plus haut).

(internes et externes), les espions (d'État ou privé), les terroristes.

Le succès d'une attaque dépendant de la compétence et de l'entraînement de son auteur, les catégories d'attaque peuvent, selon le rapport, être classées en deux grandes catégories :

- les attaques physiques, en dehors de la destruction pure et simple et de la coupure d'une ligne - non spécifique à l'informatique : interception, brouillage, écoute, balayage et piégeage.

- les attaques logiques : fouille, canal caché [18], déguisement, mystification, rejeu, substitution, faufilement, saturation, Cheval de Troie, salami, trappe, bombe, virus, ver, asynchronisme, souterrain et cryptanalyse - et la liste n'est pas exhaustive.

Un nouveau rapport du SCSSI [19] en 1997 sur l'"Introduction à la sécurité sur l'Internet" souligne qu'Internet présente trois caractéristiques majeures qui rendent difficiles l'application de certains dispositifs législatifs : la transnationalité, la fugacité et la volatilité des informations, auxquelles s'ajoutent l'évolution rapide des techniques.

Les principales menaces identifiées sont : le contournement d'un point de raccordement à Internet, l'écoute passive du réseau, l'usurpation d'identité, l'intrusion dans un routeur ou un serveur, l'importation d'un virus par téléchargement, le détournement de site et la saturation de réseau.

Ainsi, à mesure que des risques, menaces et vulnérabilités sont identifiés, des réponses sont activement recherchées et même anticipées

Dans un contexte de défense globale dans lequel la dimension non militaire de la défense a pris une ampleur nouvelle – défense civile et défense économique, il est intéressant de relire les textes constitutifs de notre arsenal juridique à la lumière de cette nouvelle donne. Nous le ferons ici pour ce qui concerne le ministère de l'Intérieur et la défense civile.

Relisons l'article 1er du décret n° 65-28 du 13 janvier 1965 relatif à l'organisation de la défense civile précisant les responsabilités du ministre de l'intérieur à la lumière de la vulnérabilité des systèmes d'information :

"Le ministre de l'Intérieur, responsable de la défense civile en application de l'article 17 de l'ordonnance du 7 janvier 1959, a pour mission, suivant les directives du Premier ministre, de :
- pourvoir à la sécurité des pouvoirs publics et des administrations publiques ;
- assurer, en matière d'ordre public, la sécurité générale du territoire ;
- protéger les organismes, installations ou moyens civils qui conditionnent le maintien des activités indispensables à la défense et à la vie des populations ;
- prendre, en matière de protection civile, les mesures de prévention et de secours que requiert en toutes circonstances la sauvegarde des populations ;
- entretenir et affermir la volonté de résistance des populations aux effets des agressions."

On constate qu'aujourd'hui les systèmes d'information interviennent dans les quatre secteurs concernés par le décret et constituent donc un élément majeur de l'esprit de défense, c'est-à-dire la cinquième mission. Et on peut considérer que ces quelques pages tendant à démontrer la vulnérabilité des systèmes d'information et la responsabilité de tous pour la réduire constituent d'une certaine façon une contribution à cette mission.

III. QUELQUES PISTES DE REFLEXIONS ET PROPOSITIONS D'ACTIONS

Si la démonstration proposée est un tant soit peu convaincante, on peut et on doit - tous - s'interroger sur les mesures à prendre. C'est pourquoi nous suggérons ci-après quelques pistes de réflexion et quelques propositions d'action.

Il faudrait sans doute tout d'abord replacer les cybermenaces dans un contexte global et admettre que nous sommes dans une situation de guerre de l'information.

18 Le canal caché permet de faire fuir de l'information en violant la politique de sécurité. Ces attaques sont perpétrées dans les systèmes ou les bases de données à plusieurs niveaux de confidentialité.

19 N° 2133, 12 décembre 1997, pp. 25.

Dans ce contexte, il est nécessaire d'informer et de sensibiliser.

Mais, il ne faut pas créer de panique ou de psychose à l'intérieur du pays ni attaquer ouvertement un autre pays et risquer un incident diplomatique. Et il faut choisir son support d'information, son mode de communication, son public cible et le moment de l'intervention : une grande campagne de "publicité" sur la vulnérabilité des systèmes d'information ? un grand discours politique de "doctrine" sur les enjeux de la société de l'information ?

Il est aussi nécessaire de former à la sécurité et de responsabiliser tous les acteurs des systèmes d'information, depuis la recherche, la conception et le développement jusqu'à l'utilisation (informatique, bureautique et ludique), depuis le cadre jusqu'à l'agent d'exécution, dans les administrations, les entreprises, le système éducatif, auprès des consommateurs etc. en mettant en avant dans toutes les structures, publiques et privées, l'importance du rôle des responsables de la sécurité des systèmes d'information (les RSSI).

Il faut donc lier obligatoirement toute initiative d'informatisation à une sensibilisation aux aspects de sécurité et inclure explicitement dans les programmes pédagogiques des formations d'informaticiens les aspects de sécurité des systèmes,

Enfin, il faut coordonner et mettre en synergie les efforts, y compris le renseignement et donc l'intelligence économique, créer un esprit d'équipe, créer un nouveau lien "armée-nation" autour d'un nouveau combat, avec de nouveaux soldats, transformer le concept de défense passive en **défense active.**

Parallèlement, il est indispensable, comme a commencé de le faire le Conseil d'État dans son récent rapport sur *Internet et les réseaux numériques* (1998), de recenser l'arsenal juridique français, communautaire et international pertinent et de le compléter si nécessaire, en prenant en compte l'intégration croissante du droit national et du droit communautaire ainsi que les interactions économiques des entreprises multinationales.

Avec son grand programme d'action, « Préparer l'entrée de la France dans *la société de l'inform@tion* » (PAGSI), 1998, diffusé sur Internet et décliné ensuite par ministères [20], l'État français veut mobiliser, sensibiliser et impulser un nouveau souffle. La récente circulaire du Premier ministre relative aux mesures à prendre pour éviter le « *bug* de l'an 2000 » [21] s'inscrit dans la même logique volontariste : on combat mieux ce que l'on connaît. La société de l'information est une extraordinaire opportunité. La France doit y jouer pleinement son rôle, avec détermination mais aussi et surtout vigilance.

A. A.-P.

20 le rapport du ministère de l'intérieur a été remis au secrétariat général du gouvernement le 15 juillet 1998.
21 Cf. Annexe.