Centre de recherche sur la sécurité et le renseignement

RENSEIGNEMENT ET SÉCURITÉ DANS L'ÂGE DE L'INFORMATION: LES DÉFIS DU QUÉBEC

par Pierre Cloutier ll.m.
avocat

Je n'apprendrai rien à personne en vous disant que nous sommes entrés depuis quelques années dans une ère nouvelle que certains spécialistes appellent la "Société de l'information", ou l'Âge de l'information" ou encore la "Société globale" ou "l'Ère du savoir" ou, pour faire revivre une vieille expression chère au regretté professeur torontois Marshall MacLuhan, le "Village global".

A n'en point douter, il s'agit dans les faits d'une véritable révolution aussi importante que celle qui a vu l'humanité passer de l'âge de l'agriculture à l'âge industriel.[1]

Comme toute révolution, ce phénomène, que le futurologue américain Alvin Toffler appelle la "Troisième vague", entraîne avec elle des changements dont nous commençons à peine à réaliser l'ampleur. Nous savons cependant que ces changements sont profonds, structurels, fulgurants et mondiaux.

Dans un texte admirable, M. Philippe Quéau, responsable du programme Imagina à l'Institut National de l'Audiovisuel de France[2], s'exprime comme suit:

> *L'ère cyber inaugure une transformation culturelle majeure dont les secousses se feront sentir longtemps dans le siècle prochain. Elle annonce aussi un bouleversement économique et social auquel nous ne sommes sans doute pas prêts. L'effacement virtuel des frontières entre les pays, l'apparition progressive de formes radicales de télétravail, à l'aide par exemple des communautés virtuelles de clones 3D, l'exploitation par les entreprises de toutes les ressources de la délocalisation des capitaux et des capacités de production, vont constituer un choc frontal pour les organisations habituées à des environnement stables ou de produits matériels, tangibles. Nous assistons déjà à une virtualisation de pans entiers de l'économie de l'information. Dans un monde de plus en plus saisi par l'immatériel, des notions comme celles de la "valeur" des choses ou du travail vont devoir être reconsidérées hardiment.*
>
> *Nous vivons une révolution profonde, comparable dans le domaine de l'information à la révolution industrielle du 19ème siècle, provoquée par la disponibilité*

soudaine d'une énergie abondante et bon marché. De même, grâce aux inforoutes et aux interfaces graphiques dont Mosaic et le fameux World Wide Web nous donnent un avant-goût, toute la mémoire du monde sera aisément accessible par tous et en tous lieux, pour un prix modique.

Lors d'une conférence ministérielle tenue à Bruxelles les **25** et **26 février 1995**, les pays du **G-7** ont adopté sensiblement le même point de vue. Dans le texte final de la conférence, on lit ce qui suit:[3]

Les progrès réalisés dans les technologies de l'information et de la communication sont en train de changer radicalement la façon dont nous vivons; comment nous travaillons et faisons des affaires, comment nous éduquons nos enfants, étudions et faisons de la recherche, comment nous apprenons et comment nous nous perfectionnons. La société de l'information affecte non seulement la façon dont les gens interagissent mais forcent également les structures organisationnelles traditionnelles à devenir plus flexibles, plus participatives et plus décentralisées.

Je vous souligne en passant que j'ai obtenu ces documents grâce au réseau Internet. Dans le cas du G-7, j'ai eu accès aux documents le lendemain de la fin de la conférence, soit le **27 février 1995**.

Chez nous au Québec, le Conseil de la Science et de la Technologie a fait le même constat.[4] Dans un document intitulé "Miser sur le savoir", publié en octobre 1994, le Conseil fait remarquer que "le monde est entré de plain-pied dans l'ère du savoir et les nouvelles technologies de l'information y jouent un rôle clé, que ce soit dans la production de la connaissance ou dans sa diffusion".

Le Conseil ajoute ce qui suit:

> *Tous les groupes, entreprises, travailleurs, médias, gouvernements, services publics sont visés. Ils doivent:*
> - *prendre conscience de l'importance stratégique des nouvelles technologies de l'information dans toutes les sphères de l'activité sociale et économique;*
> - *apprivoiser ces technologies;*
> - *s'organiser pour en tirer parti au maximum;*
> - *gérer intelligemment leur utilisation;*
> - *les mettre au service du développement social et économique du Québec.*

L'auteur américain Winn Schwartau[5] ajoute même que l'Âge de l'information a officiellement commencé le jour où notre dépendance aux ordinateurs, aux systèmes de télécommunications et aux objets de haute technologie a dépassé notre capacité de vivre sans eux.

Le vice-président senior de la compagnie multinationale Microsoft, M. Nathan Myhrvold, parle lui d'une révolution digitale[6]:

> *Bientôt, dit-il, les réseaux digitaux vont permettre aux gens d'acheter n'importe quoi, de rencontrer n'importe qui et de faire des affaires, dans un vaste marché virtuel mondial. La monnaie digitale va transformer les opérations bancaires régionales en opérations mondiales. Les pays du Tiers-Monde vont avoir accès à des marchés auxquels ils n'auraient jamais pu rêver auparavant.*

Telle une vague de fond, cette révolution s'attaque aussi au coeur même des États en imposant un nouvel ordre mondial et en remettant également en cause ses structures, y compris celles concernant le renseignement et la sécurité. Nous allons faire le tour de ces concepts en commençant par le renseignement pour nous attaquer ensuite aux questions de sécurité.

I - LE RENSEIGNEMENT

Je vais commencer par quelques constats de base. Premièrement, il ne fait aucun doute maintenant que l'effondrement du monde communiste symbolisé par la chute du Mur de Berlin est un événement significatif qui a institué de nouveaux rapports de force entre les pays en instaurant progressivement une nouvelle économie libérale mondiale qui s'impose à tous.

Deuxièmement, dans cette nouvelle économie mondiale, on sait que la concurrence est farouche voire même déloyale et les alliances militaires ne veulent souvent rien dire. A vrai dire nous sommes entrés dans un état de guerre froide permanent où le champ de bataille n'est plus exclusivement militaire mais également civil et surtout économique. La récente "guerre du flétan noir ("turbot") entre le Canada et la Communauté économique européenne (C.E.E.) est un exemple particulièrement éloquent.

Troisièmement, dans cette nouvelle économie mondiale, le savoir et la connaissance, c'est-à-dire en bout de ligne l'information, est la ressource naturelle de base, la matière première principale ou encore pour employer l'expression de M. Philippe Quéau, l'énergie abondante et bon marché. La force cérébrale a remplacé la force musculaire de l'âge industriel.[7] Comme le dit si bien Winn Schwartau[8], nous sommes engagés maintenant dans une partie mondiale de Monopoly dans laquelle l'information est la monnaie d'échange.

Dans son livre intitulé: "La nouvelle économie",[9] l'économiste canadienne Nuala Beck démontre de brillante façon que les nouvelles industries stratégiques et motrices, c'est-à-dire celles qui propulsent l'ensemble de l'économie sont celles axée sur la technologie et une haute concentration de capacité intellectuelle comme:

- les ordinateurs et les semi-conducteurs (y compris logiciels et services informatiques);
- les soins de santé (y compris médicaments, bio-médecine, fournitures et matériel médicaux et chirurgicaux);
- les communications et les télécommunications (y compris matériel de fusées et d'appareils astronautiques, communications radio, micro-onde et divertissement);
- l'instrumentation (contrôle de processus, matériel et conseil axés sur l'environnement, instruments optiques et lentilles, matériel d'ingénérie et scientifique).

Le Conseil de la Science et de la Technologie tient sensiblement le même discours[10]. Parlant de l'ère du savoir, le Conseil mentionne ce qui suit:

> *La connaissance a toujours joué un rôle dans l'économie, sous la forme de savoir-faire empirique. Ce qui apparaît plus nouveau aujourd'hui, c'est que la valeur ajoutée des biens et des services repose de plus en plus sur le savoir qu'on y injecte. La connaissance ne fait pas que s'ajouter aux autres facteurs de production, elle oriente le choix des autres facteurs comme les matières premières ou les procédés de transformation, elle se retrouve dans la machinerie utilisée ainsi que dans la qualité de la formation des employés et dans les stratégies des chefs d'entreprise. De plus en plus, c'est la nature des connaissances d'un bout à l'autre de la chaîne qui différencie les produits entre eux et qui, en fin de compte, détermine les gagnants.*

Cela étant dit, une conclusion évidente s'impose: si d'une part les individus, les organisations et les pays sont engagés à l'échelle mondiale dans une guerre froide économique permanente et que d'autre part la connaissance, le savoir et en bout de ligne l'information est la matière première de cette économie, force nous est donc de conclure que les meilleurs seront ceux qui seront mieux "armés" ou mieux équipés pour livrer la bataille de la connaissance et du savoir,

c'est-à-dire en bout de ligne de faire face adéquatement à la guerre permanente et totale de l'information.

Pour bien comprendre les enjeux, il faut toutefois bien comprendre les concepts. Quand on parle de savoir, de connaissance et en bout de ligne d'information, on parle somme toute de quelque chose qui a toujours existé et qui existera vraisemblablement toujours puisqu'elle est reliée à la production intellectuelle de l'être humain. Ce qui est nouveau toutefois aujourd'hui c'est la façon dont ce savoir, cette connaissance et cette information est stockée et diffusée.

Le développement fulgurant et rapide de l'informatique (Schwartau utilise l'expression: "Computers Everywhere") et des télécommunications et leur interconnexion dans un réseau global (en anglais "Global Network") ont ajouté en effet deux éléments nouveaux et inédits: d'abord la quantité absolument hallucinante d'informations disponibles et la vitesse fulgurante avec laquelle ces informations sont diffusées à travers la planète.

En fait, jamais dans l'histoire de l'humanité, des individus et des groupes d'individus n'ont eu accès, comme maintenant, à une telle quantité et une telle qualité de connaissances, d'informations et de renseignements stratégiques.

Pour bien comprendre cette réalité, il faut préciser toutefois que le mot "information" lui-même est un concept général et parfois ambigu qui renvoie en réalité à trois (3) notions qui sont fort différentes les unes des autres: il faut en effet faire une distinction entre les termes "données" (en anglais "data") "information" (en anglais "information") et "renseignement" (en anglais "intelligence").[11]

Les "données" sont les textes bruts, les images, les sons et de façon générale les signaux électromagnétiques. L'information est un agencement de données d'intérêts communs, comme on en retrouve dans les médias ou les rapports de recherche. Le "renseignement" , par contre, est

défini comme de: "l'information analysée et évaluée afin de permettre à une personne spécifique de prendre une décision spécifique concernant un sujet spécifique à un endroit et à un moment spécifique".

En fait, le mot "renseignement" n'a de sens que s'il est utilisé dans un contexte d'aide à la décision (en anglais "decision support").

C'est là que ça devient intéressant. On peut affirmer sans se tromper que plus la capacité de stockage des données augmentera, plus l'information sera grande. Plus l'information sera grande, plus les capacités de renseignement augmenteront également, améliorant de ce fait même la qualité de l'aide à la décision et en bout de ligne la compétitivité des individus, des organisations et des pays.

D'autre part, plus la vitesse de diffusion des données sera grande, plus l'information sera rapide. Plus l'information sera rapide, plus les renseignements seront accessibles rapidement et plus les décisions seront prises rapidement améliorant encore là et par ce fait même la compétitivité des individus, des organisations et des pays. On peut penser facilement que les gagnants seront ceux qui seront les plus rapides à transmettre les renseignements utiles à la prise de décision.

Pour vous donner une idée de ce qui s'en vient, je vous renvoie au tableau publié dans la revue américaine "Business Week"[12] du 24 janvier 1995 à la page 150 et compilé grâce aux données fournies par des compagnies comme American Telephone and Telegraphe (AT&T) et International Business Machine (IBM). Sans entrer dans les détails, qu'il suffise de mentionner que d'ici l'an 2010, la capacité des ordinateurs personnels passera de 3 millions de transistors (50 millions d'opérations à la seconde) à 250 millions de transistors rendant possible, entre autres, la diffusion d'images en trois (3) dimensions dans des vidéo-conférences.

Des logiciels "intelligents" assureront la gérance de réseaux informatiques trop complexes

pour l'être humain et la production sera entièrement automatisée. Les transistors auront la grosseur de quelques atomes et les disques compacts seront remplacés par des petites disquettes pouvant stocker des librairies entières de textes, d'images et de sons.

La vitesse de transmission se mesurera en trillions de "bits" par seconde dans un réseau mondial composé de fibres optiques, de satellites et de communications sans fil. 90% du trafic sera multimédia (textes, images et sons).

On peut donc déduire sans se tromper beaucoup que d'ici les 20 prochaines années, ce que j'appelle, moi, la "capacité informationnelle" des individus, des organisations, des sociétés, des peuples, des nations ou des pays augmentera considérablement. Comme cette "capacité informationnelle" est la voie royale à travers laquelle passent la connaissance, le savoir et le renseignement stratégique, qui sont les forces motrices de la nouvelle économie mondiale, il est fort à parier que la richesse collective augmentera.

L'accès égalitaire de tous les individus, les organisations et les pays à cet espace infini que les Américains appellent "Cyberspace"[13] est évidemment une question politique majeure et un principe qui a été reconnu par les pays du G-7 lors de la Conférence de Bruxelles[14].

Cependant point n'est besoin de posséder un doctorat en économie pour comprendre que certains individus, certains groupes ou certains pays seront évidemment plus "égaux" que d'autres. Si on parle de marché global, certains insisteront pour parler bientôt de social-démocratie mondiale. Si on parle de richesse collective mondiale, certains avanceront qu'on devra parler également de redistribution équitable de cette richesse à l'échelle mondiale. Mais il s'agit là d'un autre débat.

Dans une optique de saine compétitivité toutefois, on peut analyser les choses autrement. Les individus, les organisations et les pays les meilleurs seront ceux qui seront capables d'harnacher le mieux la richesse informationnelle disponible pour la transformer en renseignements

stratégiques facilitant la prise de décision. Le meilleur exemple d'un pays qui a réussi à faire cela magnifiquement est le Japon.

Qu'il suffise de mentionner à titre d'exemple que, selon les propos tenus par le professeur Juro Nakagawa de la Faculté de commerce de Aichi Gakun au Japon, les compagnies commerciales japonaises sont le fer de lance de la capacité de renseignement économique du Japon et que ces compagnies recueillent l'équivalent de 6,000 pages d'informations chaque jour à travers le monde.[15]

En fait, force nous est de constater que l'essor absolument phénoménal du Japon est le résultat direct de la mise sur pied après la Seconde Guerre Mondiale d'une structure extrêmement efficace de renseignement économique et commercial, appelée l'Organisation japonaise du commerce extérieure (en anglais Japan External Trade Organisation - JETRO)[16]

Selon M. John Quinn, un ex-officier de renseignement de la C.I.A., spécialiste du Japon:

- Les organisations japonaises de renseignement se divisent en deux (2) secteurs; le gouvernement japonais et le secteur privé;
- Les agences gouvernementales japonaises sont relativement petites. Le Japon n'a pas de super agence centralisée de renseignement comme la C.I.A.;
- Les besoins en renseignement du Japon sont essentiellement de nature économique et la majeure partie de la collecte, de l'analyse et de la distribution du renseignement est effectuée par le secteur privé;
- Il y a une interaction constante entre le gouvernement japonais et le secteur privé;
- Les efforts portent principalement sur le renseignement commercial, économique et technologique.

Cela m'amène à vous dire que de façon générale, la cueillette du renseignement à l'échelle mondiale se fait de deux (2) façons: de manière clandestine ou de manière ouverte. Quand cette

cueillette se fait de manière clandestine, on parle alors d'espionnage. Mon collègue René Hébert, avec qui je collabore depuis cinq ans et avec qui j'ai fondé notre modeste Centre de recherche sur la sécurité et le renseignement, fera le tour de la question et je n'ai pas l'intention de le recouper.

Je voudrais par contre insister sur l'utilisation massive, systématique et disciplinée des sources ouvertes d'informations et leur transformation en renseignements stratégiques utiles à la prise de décision.

Jusqu'à tout récemment seules les grandes organisations - en majeure partie étatiques - avaient les moyens de recueillir - la plupart du temps clandestinement - les renseignements stratégiques dont les États avaient besoin pour leur sécurité et leur compétitivité.

L'interconnexion des banques de données publiques et privées entre elles et surtout l'expansion foudroyante des réseaux internationaux de communications "ouverts" comme l'Internet est venu complètement changer les règles du jeu.

Le premier à s'en rendre compte aux États-Unis fut l'ex-agent de renseignement Robert David Steele. Les circonstances entourant cette prise de conscience méritent ici d'être relatées.[17]

Haut fonctionnaire civil et spécialiste du renseignement et de l'informatique, Steele fut chargé en 1988 de mettre sur pied le Centre de renseignement du Corps des Marines des Etats-Unis (US Marine Corps Intelligence Center) avec un budget initial de 20 millions$.

Quelques mois après le début des opérations, Steele réalisa - et ce fut tout un choc pour lui - que son système informatique sophistiqué, hypersecret et branché sur les banques de données des super agences étatiques de renseignement américaines comme la Central Intelligence Agency (CIA), la National Security Agency (NSA) et la Defense Intelligence Agency (DIA) ne lui servait pratiquement à rien.

En effet, même si ces bases de données contenaient des milliers d'informations sur le nombre d'ogives nucléaires soviétiques, elles ne contenaient, entre autres, aucune information utile sur les pays du Tiers-Monde, dont le Marine Corps avait un urgent besoin pour être en mesure d'intervenir efficacement dans ces pays, comme, par exemple, la Somalie.

Par contre, Steele a réalisé que l'utilisation d'un simple ordinateur personnel avec un modem lui donnant accès aux banques d'informations privées comme LEXIS-NEXIS, EASYNET ou JANE'S INFORMATION GROUP, à un coût annuel d'environ 20,000$ lui permettaient sans aucune difficulté de rencontrer la majeure partie des besoins en renseignements du Corps des Marines. Steele inventa alors le concept de Open Source Intelligence ou OSCINT.

Selon Steele, 80 % des renseignements dont les états ont besoin pour assurer leur sécurité et leur compétitivité se retrouvent dans le secteur privé et sont facilement accessibles. (Ce pourcentage est de 95% en ce qui concerne les entreprises privées). L'accès généralisé à un réseau ouvert comme Internet vient encore plus renforcer ce postulat en lui conférant une dimension individuelle et universelle.

A ce stade-ci, je me permets donc de tirer quelques conclusions intérimaires:

1- Le renseignement n'est pas et n'est plus l'apanage exclusif des états et des gouvernements. Les grandes agences gouvernementales comme la CIA, le MI6 ou la NSA ne sont plus les seuls à produire du renseignement et constitueront probablement même dans l'avenir des groupes minoritaires.

2- Le renseignement n'est pas non plus l'apanage exclusif des organisations privées ou publiques. Avec le développement de ce que Winn Schwartau appelle le "Global Network", chaque individu deviendra non seulement un consommateur mais aussi un producteur de renseignement. Ce fait a été reconnu par M. Ward Elcock, le nouveau directeur du Service canadien de renseignement de sécurité, qui a mentionné récemment[18], "que chaque citoyen sera ou aura la capacité dans l'avenir de devenir un

officier de renseignement".

3- Le renseignement n'est plus relié exclusivement aux questions de sécurité nationale. On assiste actuellement à une explosion sans précédent de nouveaux créneaux dans toutes les sphères de l'activité humaine. On parle désormais de renseignement d'affaires (business intelligence), de renseignement économique (economic intelligence), de renseignement diplomatique (diplomatic intelligence), de renseignement touchant le respect de la loi (law enforcement intelligence), de renseignement touchant la protection civile (Operations others than war Intelligence), de renseignement touchant le maintien de la paix (Peacekeeping Intelligence), de renseignement politique (Political Intelligence), de renseignement touchant l'environnement (Environmental Intelligence), etc.

En fait, si on accepte la définition que j'ai mentionnée précédemment, on peut affirmer avec assez de certitude que le renseignement, c'est-à-dire l'information analysée et évaluée portant sur un sujet précis, destinée à une personne précise, à un moment et à un endroit précis pour l'aider à prendre une décision importante la concernant ou concernant son organisation ("decision support") sera utilisée massivement dans l'avenir pour permettre à ces individus ou organisations de se développer et de demeurer compétitifs dans leur créneau d'expertise ou dans leur marché.

Cette définition s'applique non seulement à tous, comme je viens de le dire, mais également à tous les niveaux hiérarchiques des organisations quelles qu'elles soient: associations avec ou sans but lucratif, compagnies privées, organismes publics, gouvernements, états, nations, organismes internationaux, etc.

D'autre part, comme le mentionne Robert Steele[19] dans l'Âge de l'information, le "renseignement" est beaucoup moins une question de pénétration des secrets que l'art de trouver l'information utile à travers le flux constant et illimité d'informations ouvertes qui sont disponibles légalement et à bas prix, particulièrement en ce qui concernent les sources électroniques.

Selon lui, les coûts politiques et économiques de l'espionnage industriel ou de l'inflitration clandestine des autres gouvernements ou pays dans le but de connaître leurs plans et intentions sont astronomiques et hors de proportion, lorsqu'on les compare avec le renseignement provenant de sources ouvertes.

Il estime également que le concept de la centralisation du renseignement, comme on le connaît aujourd'hui - la C.I.A. est le meilleur exemple - ne peut pas survivre dans l'Âge de l'information. Il affirme, en effet, qu'en mettant l'accent sur le renseignement provenant de sources ouvertes (OSCINT), une nation ou un pays peut mobiliser chacun de ses secteurs d'excellence et se transformer en une immense agence nationale "virtuelle" de renseignement ayant des capacités de cueillette, d'analyse et de distribution, de loin supérieures à celles fournies actuellement par les agences bureaucratiques de l'État qui s'occupent de la sécurité nationale.

La solution réside donc pour lui dans la création, à l'intérieur d'un pays donné, de cette communauté virtuelle de l'information (en anglais "National Information Continuum") composée de neuf(9) grands secteurs de la société: les écoles et collèges, les universités, les bibliothèques, les entreprises privées, les courtiers en informations et les agences de sécurité privées, les médias, les gouvernements, l'armée et les agences étatiques de renseignements.

En fait si on suit ce raisonnement, le véritable défi des sociétés modernes dans l'Âge de l'information sera de trouver les moyens les plus efficaces et les plus performants pour harnacher l'information publique disponible pour la transformer en renseignement stratégique utile à leur sécurité et à leur compétitivité.

Comme vous vous en doutez peut-être, les Japonais sont déjà dans le coup s'il faut en croire les propos tenus par M. Shojiro Asai, directeur général du "Advanced Research Laboratory" de la compagnie Hitachi. Interrogé par la revue américaine Business Week[20], M. Asai a mentionné clairement que sa compagnie mettait l'accent sur l'utilisation des ordinateurs guidés par des

logiciels de reconnaissance de la voix et "d'agents intelligents" (en anglais "intelligent agents") programmés pour parcourir le réseau Internet afin d'en extraire les informations utiles.

En guise de conclusion générale pour ce premier chapitre, je me contenterai de souligner que s'il y a un avenir pour le Québec, particulièrement sur le plan économique, c'est dans la solution proposée par Steele qu'elle se trouve et cela pour plusieurs raisons:

1- Nous n'avons pas vraiment le choix. Dans une économie globale où l'information est à la fois le substitut du temps, de l'espace, du capital et du travail et surtout une forme d'énergie inépuisable et à bon marché, le Québec ne pourra survivre à moins de devenir une "nation intelligente" (en anglais a "smart nation"), c'est-à-dire une nation à la fine pointe du savoir, de la connaissance et en bout de ligne de la maîtrise de l'information.

2- Dans le cadre du partage actuel des compétences à l'intérieur de la fédération canadienne, il n'y a absolument aucun risque pour le Québec, sur le plan politique, à suivre cette voie. L'harnachement des sources ouvertes d'informations, notamment dans les secteurs économique (economic intelligence), des affaires (business intelligence), d'application de la loi (law enforcement intelligence), de l'environnement (environemental intelligence), de la diplomatie (diplomatic intelligence) et de la protection civile (operations others than wars intelligence), pour n'en nommer que quelques-unes, sont des activités tout à fait légitimes, légales, constitutionnelles et surtout efficaces et profitables. Le Québec doit être mesure d'utiliser toutes ses compétences au maximum et une alliance profonde entre l'État et ses partenaires sociaux-économiques est une nécessité.

3- Si le Québec devient souverain, il n'y aura plus aucun obstacle constitutionnel et il appartiendra alors au gouvernement élu d'évaluer l'hypothèse d'utiliser les sources clandestines (en anglais "covert sources") et de confier le travail à des agences spécialisées. Mais il faudra alors éviter la lourdeur bureaucratique en ayant recours à des petites unités décentralisées à la fine pointe de la technologie et à l'utilisation non négligeable des sources humaines. Il ne faut jamais oublier que la collecte de

renseignements stratégiques par des sources clandestines ne représente que 10% à 15% des besoins d'un État et que les investissements et les risques sont importants.

A ce sujet, je vous signale en passant que, selon l'auteur Peter Schweizer[21], dans son livre "Friendly Spies", les Allemands auraient mis sur pied un groupe composé de 36 spécialistes en informatique et en renseignement dont l'objectif est d'utiliser des ordinateurs sophistiqués pour pénétrer les banques de données des grandes corporations privées et des gouvernements à travers le monde, en opérant à des milliers de milles de distance. C'est le projet "Rahab".

Cette information m'amène tout naturellement à ouvrir par ce fait même le deuxième volet de mon exposé, à savoir les questions de sécurité nouvelles qui surgissent avec l'Âge de l'information.

II - LA SÉCURITÉ

Je vais commencer par une citation de Robert Steele prononcée lors d'une allocution qu'il a donnée dans le cadre de la Seconde conférence internationale sur la guerre de l'information, tenue le 19 janvier 1995 à Montréal:[22] Parlant dans une perspective militaire américaine, Steele a affirmé ce qui suit:

> *Nous sommes en guerre maintenant et quiconque ne comprend pas cela fait partie du problème. Nous sommes dans une situation de guerre totale maintenant et malheureusement pour le commandement militaire traditionnel, 99% des troupes, des armes et des équipements sont civils- ils sont "hors de contrôle".*

Je dois vous avouer bien candidement d'ailleurs qu'il y a quelques mois à peine je n'aurais pas prêté attention à ce genre de remarques, habitués que nous sommes à nous faire prédire toutes sortes de catastrophes, de désastres, de cataclysmes et de guerres.

A vrai dire, je ne pense pas que j'aurais vraiment été en mesure de comprendre ce que Steele voulait dire si je n'avais pas lu auparavant le livre de Winn Schwartau intitulé: "Information Warfare: Chaos on the Electronic Superhighway".[23] A la fin de ce livre, j'ai compris que la situation était sérieuse et que certains spécialistes en sécurité informatique américains redoutaient une attaque de grande envergure contre leurs réseaux de communications civils et militaires, c'est-à-dire ce que certains appellent un "Pearl Harbor électronique".

Je ne suis pas un informaticien ni un spécialiste de la sécurité informatique - comme bon nombre d'entre vous. Il se peut que je n'apprenne rien de nouveau à personne - et je m'en excuse d'avance - mais je vais tenter tout de même de vous résumer ce qui m'apparaît comme les choses les plus importantes à retenir. Et il y en a beaucoup, croyez-moi.

Schwartau mentionne tout d'abord que la guerre de l'information - qui est une guerre totale et mondiale - est la résultante de quatre (4) phénomènes qui ont pris naissance au cours des 30 dernières années, soit:

1- l'apparition d'un nouvel ordre mondial, basé sur une économie globale;
2- l'envahissement fulgurant des ordinateurs dans la vie de tous les jours;
3- la création d'un réseau de communications planétaire;
4- l'émergence de l'économie financière et de la monnaie virtuelle (digital cash).

Comme je l'ai mentionné dans la première partie de mon exposé, la chute du monde communiste a entraîné avec elle la fin du dirigisme économique et l'ouverture des marchés à l'échelle mondiale où tous les pays sont en concurrence les uns contre les autres. Comme l'information, c'est-à-dire la connaissance, le savoir, donc la richesse, sont les fers de lance de cette nouvelle économie, l'équation est facile et simple à faire.

La présence des ordinateurs dans la vie de tous les jours est un facteur réel depuis une vingtaine d'années. Selon Schwartau il y a environ trois (3) milliards d'ordinateurs à travers le monde qui gèrent actuellement toutes les composantes de nos vies. Ces ordinateurs ne nous apparaissent pas comme tels à première vue puisqu'ils se cachent derrière des objets courants: élévateurs, fours à micro-ondes, videos, télévisions, caméras, laveuses-sècheuses, automobiles, caisses enregistreuses, cartes de crédit, téléphones, télécopieurs, calculatrices, systèmes d'ignition et d'alarmes, cadrans, cafetières, montres digitales, feux de circulation, chronométreurs, extincteurs d'incendie, etc.

A ces trois (3) milliards, il faut ajouter les quelques centaines de millions d'ordinateurs personnels et de systèmes informatiques que l'on retrouve maintenant partout à travers le monde. Schwartau appelle ce phénomène: "Computers Everywhere".

Le réseau global ("Global Network"), lui, est le descendant direct du "Computers

Everywhere". Voici comme s'exprime Schwartau à ce sujet:

> *Le réseau global c'est le lien des ordinateurs entre eux. C'est une forme de Cyberspace, un endroit où quiconque peut voyager électroniquement et aller partout sur la planète. C'est la capacité de connecter chaque ordinateur sur n'importe lequel autre ordinateur ou connecter une personne avec n'importe laquelle autre personne. Le réseau global c'est la communication instantanée n'importe où, par la voix, par l'image et par les données. Le réseau global c'est La Grosse Compagnie de téléphone. Ce sont les satellites, les modems, les télécopieurs, le câble, la télévision interactive et les téléphones cellulaires.*

En ce qui concerne l'économie financière, elle est apparue en 1971 lorsque le président Richard Nixon a mis fin aux accords de Bretton Woods et a laissé flotter le dollar US, qui régnait en roi et maître depuis la fin de la Seconde guerre mondiale.

Depuis ce temps s'est développée en marge de l'économie réelle une économie parallèle financière qui est en fait une immense partie de poker et de gambling. Le développement de l'informatique et des réseaux de communications où se transigent des centaines de milliards d'argent digital sous formes d'opérations binaires de 0 et de 1 est venu compléter le décor. Dans cet univers hallucinant, la spéculation est la règle d'or - l'exemple le plus éloquent étant la faillite récente d'une des plus prestigieuses banques d'Angleterre, la Banque Barings. L'information - c'est-à-dire des milliards et des milliards de données, d'informations et de renseignements stratégiques stockés dans des milliers de systèmes informatiques super-puissants, analysés et communiqués instantanément à travers le monde -est le tyran qui règne en maître absolu.

Ceci étant dit, il convient maintenant de définir le théâtre des opérations -le champ de bataille si vous aimez mieux - identifier les cibles visées, connaître les guerriers, leurs armes et leurs stratégies pour pouvoir ensuite proposer des moyens de défense.

2.1 - Cyberspace

Dans l'Âge de l'information, le champ de bataille s'appelle CYBERSPACE. J'utilise volontairement le mot anglais parce que je n'ai pas encore trouvé l'expression juste en français qui me permettrait de mieux qualifier cette réalité.

Schwartau définit ce concept de la façon suivante:[24]

> *Cyberspace c'est l'espace intangible entre les ordinateurs où l'information existe momentanément lorsqu'elle voyage d'un bout à l'autre de l'espace global (en anglais Global Network). Quand un petit garçon téléphone à sa grand-mère, ils se parlent dans Cyperspace, l'espace entre les téléphones. Cyperspace c'est une réalité impalpable, une infinité d'électrons voyageant à travers des fibres de cuivre ou de verre à la vitesse de la lumière d'un point à un autre. Cyberspace inclut les ondes électromagnétiques qui vibrent à travers les communications par cellulaires, par micro-ondes et par satellite. Nous sommes branchés d'une douzaine de façons sur le réseau global et dans ce sens nous faisons tous partie de Cyberspace. Cyberspace c'est là où est tout notre argent, à l'exception de l'argent comptant que nous avons dans nos poches.*

Cyberspace est la convergence de la présence des ordinateurs dans la vie courante ("Computers Everywhere") et du réseau global ("Global Network")

Soit dit en passant, une des composantes les plus importantes de Cyberspace c'est le réseau téléphonique lui-même. Même si on pense généralement que le téléphone n'est pas un ordinateur, il faut comprendre que le système téléphonique mondial est dans les faits un immense commutateur électronique (en anglais "switch") contrôlé par ordinateur, avec des centaines de millions de terminaux (appareils téléphoniques) à travers le monde.

2.2 - Le climat

Schwartau souligne que cette guerre de l'information se déroule sur un fond de "schizophrénie binaire", cette maladie moderne qui consiste à prendre conscience de notre dépendance face aux ordinateurs mais à avouer en même temps que nous ne leur faisons pas confiance.

2.3 - Les objectifs

Quels sont les objectifs poursuivis par les guerriers de l'information? Il y en a quatre (4) selon Schwartau:

- le vol d'informations;
- la modification des informations;
- la destruction des informations;
- la destruction des systèmes informatiques.

2.3.1 - Le vol d'informations

Le vol d'informations, qui est le premier objectif de tous les guerriers de l'information, comprend, entre autres:

- le vol des secrets corporatifs (l'espionnage industriel);
- le vol des secrets militaires et des codes de communications;
- le vol des numéros de cartes de crédit, des codes d'accès, des cartes d'appels téléphoniques et des dispositifs modernes d'argent électronique;

Le vol d'informations permet également l'extorsion ou le chantage qui peuvent être utilisés par les guerriers de l'information qui possèdent des informations privilégiées sur des individus ou des organisations. Je vous réfère à ce sujet à un excellent article publié dans le numéro spécial du printemps 1995 du Time Magazine[25] où on mentionne que les crimes commis par ordinateur deviennement de plus en plus audacieux et imaginatifs sans que les lois actuelles soient vraiment en mesure de les combattre efficacement.

2.3.2 - La modification des informations

Dans l'industrie de la sécurité informatique, on parle de l'intégrité de l'information. A titre d'exemple, dans le monde financier, l'intégrité de l'information est une chose essentielle et vitale et je ne pense pas que la démontration soit difficile à faire. Une couple de zéros de plus ou de moins dans un compte bancaire peut faire toute la différence au monde. Si votre dossier de crédit comporte quelques erreurs bêtes, c'est assez pour vous causer beaucoup... d'embêtements.

Autrement dit, la modification des données est une excellente méthode pour un guerrier de l'information pour instiller la peur, causer des dommages et et faire du tort à des victimes, le tout sans avertissement.

Les dommages sont encore plus grands lorsqu'ils sont affligés à des corporations dont les données vitales sont faussées.

2.3.3 - La destruction de l'information

La destruction des informations est un excellent moyen pour un guerrier de l'information de camoufler un vol. C'est une porte de sortie efficace qui rend encore plus compliquée le processus d'enquête et de restauration des données.

2.3.4 - La destruction des systèmes informatiques

Nous savons tous comment les réseaux d'information et de communications sont essentiels à l'existence même des organisations et à la sécurité économique des pays. Le guerrier de l'information peut décider un matin qu'il est stratégiquement rentable pour lui de détruire tout possibilité pour son adversaire de traiter la moindre information en détruisant complètement son système informatique. Selon Schwartau des armes de destruction massive de systèmes informatiques sont maintenant disponibles sur le marché à des coûts très peu élevés et ces armes peuvent faire des dommages considérables.

2.4 - Les caractérisques des armes utilisées

Avant de parler de la panoplie des armes utilisées par les guerriers de l'information, il convient de mentionner que ces armes sont par essence insidieuses, invisibles, passives, téléguidées à distance, et désastreuses.

Elles sont insidieuses parce qu'elles opèrent à l'improviste. Elles sont invisibles parce qu'elles sont difficilement repérables. Elles sont passives parce qu'elles peuvent "dormir" pendant longtemps à l'intérieur d'un système puis exploser à un moment prévu. Elles sont téléguidées parce qu'elles peuvent être manipulées à des milliers de kilomètres de distance et enfin elles sont désastreuses parce qu'elles peuvent faire des dommages considérables.

2.5 - Les armes utilisées

2.5.1 - Les virus informatiques

La première pièce d'équipement utilisée dans Cyberspace et la plus importante est évidemmment le logiciel. Sans logiciel pas d'ordinateurs et pas de réseau global. Le logiciel c'est le cerveau derrière les systèmes informatiques mondiaux. C'est ce qui permet au réseau global de vivre et de respirer à travers Cyberspace. Cependant, très peu de gens sont vraiment conscients de l'importance des logiciels pour la sécurité économique et militaire des pays.

Il faut comprendre toutefois au départ que les logiciels ne sont dans les faits que des séries d'instructions mathématiques complexes et d'opérations binaires sophistiquées qui, même s'ils réalisent tous les jours des exploits remarquables, sont essentiellement vulnérables et susceptibles à tout moment "de se planter", pour employer une expression consacrée.

Cette proposition vient tout simplement de l'application simple d'un théorème mathématique fort connu, celui du philosophe allemand Kurt Goedel qui veut que toutes les formulations axiomatiques cohérentes de la théorie des nombres incluent des propositions indécises (en anglais "undecidable"). Et évidemment, plus les logiciels sont compliqués plus des erreurs sont susceptibles d'intervenir.

Quand les erreurs sont provoquées délibérément, on appelle cela des virus informatiques. Je ne vous apprendrai rien en vous disant que le virus informatique est la première arme utilisée par les guerriers de l'information qui sont bien au courant de la vulnérabilité des logiciels.

Sans entrer dans les détails qu'il suffise de mentionner qu'en 1987 il y avait seulement six (6) virus identifiés. En 1990, il y en avait 1 000. En 1993: 3000. Comme le dit si bien Bernard Derome, "si la tendance se maintient", il y a aura bientôt 100,000 virus qui se baladeront librement dans Cyberspace. C'est évidemment un problème majeur qui n'a pas fini de causer des soucis constants.

2.5.2 - Les "renifleurs" de réseau

En anglais, on les appele les "sniffers". Les cibles: les systèmes informatiques, les téléphones, les téléphones cellulaires, les télécopieurs et les satellites de communications. Les objectifs: pénétrer illégalement dans les systèmes, voler les informations intéressantes, les détruire, chercher les mots de passe et les codes d'accès, intercepter les conversations et ultimement rendre les systèmes inopérables.

Les moyens utilisés sont simples et fort peu coûteux:

- les "analyseurs de réseaux" (en anglais "network analyser") utilisés pour diagnostiquer et aider à la réparation des réseaux locaux. Un outil efficace de travail pour les administrateurs de réseaux, mais une arme redoutable entre les mains des guerriers de l'information. Le dernier en date s'appelle Satan et a été mis au point par un jeune programmeur aux cheveux longs, Dan Farmer,[26] qu'il l'a rendu disponible sur le réseau Internet malgré l'opposition de son employeur qui l'a foutu à la porte.
- les logiciels spécialement conçus pour faire ce travail et qui sont à la portée de tout le monde. L'underground cybernétique contient un nombre important de ces programmes, dont le "IPX Permissive" qui permet aux intrus de lire et de décoder les données des réseaux Novell.
- une autre méthode consiste à se brancher directement sur les fils des réseaux et y collecter les informations soit directement ou encore indirectement (passive sniffing) en utilisant un inducteur qui recueille les fluctuations magnétiques provoquées par le flux de données et qui les reconvertit en signaux électriques. On peut utiliser aussi un petit transmetteur radio pour communiquer à distance les données et les mots de passe.

Comme vous le savez tous, malgré les mesures de protection prises par les administrateurs,

les réseaux informatiques locaux sont extrêmement vulnérables et le développement d'un réseau de réseaux comme Internet vient encore plus compliquer les choses. Internet est composé d'environ deux (2) millions d'ordinateurs serveurs ("host computers") et permet l'accès à des millions d'autres ordinateurs. Presque tous les pays de la plantète ont au moins une connection Internet et il y a environ 100,000 millions de bytes de données qui traversent le réseau tous les jours. Avec une augmentation de 15% par mois et de 50% tous les six (6) mois, le réseau est déjà plein. Et ça ne fait que commencer.

D'autre part, le réseau téléphonique - que les Américains appelle la "Switch" - est depuis longtemps la cible préférée des guerriers de l'information. Comme je l'ai mentionné précédemment, la "Switch" est dans les faits le plus gros ordinateur et le plus gros réseau au monde et aussi le plus facile à utiliser.

Le contrôle de la "Switch" représente un immense pouvoir. C'est là que sont entreposés les factures, les paiements effectués, les adresses et tous les autres renseignements personnels concernant tous les abonnés. Chaque appel que l'on fait, chaque appel que l'on reçoit est enregistré. Même les renseignements concernant les abonnés non inscrits s'y trouvent.

Une fois qu'un guerrier de l'information a accès à la "Switch" il peut intercepter toutes les conservations intérieures et internationales.

Les guerriers de l'information se servent également de logiciels pour déterminer quels sont les numéros de téléphones qui sont connectés à un téléphone et ceux qui sont connectés à des ordinateurs. On appelle ces logiciels les "Demon Dialer", qui sont en fait des dispositifs artisanaux composées de pièces détachées électroniques peu dispendieuses et terriblement efficaces, comme le sont toutes les "boîtes de couleurs" ("Colored Boxes") utilisés par ceux que les Américains appelent les "hackers" (en français "pirates") et les "phone phreaks" (intraduisibles) depuis de nombreuses années.

Pour les curieux, qu'il suffise de mentionner que tous les trucs utilisés par les "hackers" sont accessibles sur le réseau Internet, soit par des serveurs comme celui de Phrack Magazine (adresse internet: <http://freeside.com/phrack.html>) où vous pouvez télédécharger (en anglais "downloading") les 46 numéros de la revue qui existe depuis le 17 novembre 1985, ou encore sur CDROM, comme le "Hacker's Chronicle", disponible sous le comptoir à Montréal et qui en est rendu à son troisième volume.

Les télécopieurs sont encore plus vulnérables. Selon Schwartau, une industrie entière s'est développée aux USA à partir des produits développés pour intercepter les transmissions des télécopieurs. Schwartau cite des compagnies comme Burlex International, Mentor Links, Sherwood Communications, El-Tec International et Knox Security Engineering.

Les communications sans fil ne sont pas non plus à l'abri. Les conversations téléphoniques cellulaires sont extrêmement vulnérables et on peut facilement acheter l'équipement nécessaire pour un prix ridicule (environ 200,00$) dans des endroits comme Radio-Shack. Qui ne souvient pas de l'incident Wilhemny-Tremblay pendant la campagne référendaire de 1992?

La fraude cellulaire est également une pratique largement répandue aux États-Unis et possiblement au Canada. Quand on fait un appel, chaque téléphone cellulaire diffuse également son numéro de série électronique interne (en anglais "Electronic serial number" ou ESN). Ce numéro sert à authentifier l'appel en vérifiant le numéro de téléphone et la facturation. Ce numéro est périodiquement retransmis avec d'autres informations critiques rendant l'interception relativement simple. Le guerrier de l'information peut ainsi intercepter tous les renseignements utiles pour lui permettre d'utiliser l'appareil et de faire facturer les frais à l'abonné.

Schwartau explique que dans les grandes métropoles américaines, des fraudeurs se promènent en limousines dans les quartiers immigrants défavorisés et offrent des appels interurbains internationaux à des prix ridiculement bas. L'appel est évidemment chargé aux

abonnés qui ne se doutent de rien et comme la limousine se déplace constamment elle devient difficilement repérable.

Les communications par satellites sont aussi interceptables. Schwartau mentionne à ce sujet que le 27 avril 1986, les auditeurs du réseau HBO câblé ont vu apparaitre sur leur écran de télévision pendant la diffusion d'un film, une annonce d'un certain "Captain Midnignt" protestant contre le coût excessif de l'abonnement. En fait, dit Schwartau, le signal satellite de la station avait été intercepté par un hacker en désaccord avec le brouillage de la télévision payante.

Soulignons en terminant ce chapitre que la fraude électronique coûte des milliards de dollars. Une étude réalisée aux USA en 1991 évalue à 8 893 000,000$ les fraudes électroniques de toutes natures et ce chiffre ne tient pas compte de ce qui se passe sur le réseau Internet.

2.5.3 - Le monde de Monsieur Van Eck

En **1985**, le professeur hollandais Win Van Eck a publié dans une revue spécialisée un article intitulé: "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?[27] Dans cet article, le professeur hollandais expliquait essentiellement que les ordinateurs, les imprimantes, les télécopieurs, les écrans vidéo sont aussi des dispositifs électriques qui conduisent le courant et qui émettent des champs magnétiques. Ces champs magnétiques peuvent être interceptés à distance par un appareil récepteur simple - comme un téléviseur en noir et blanc et quelques pièces additionnelles bon marché - et être lus parfaitement, de façon invisible et passive et avec très peu de chances d'être repéré.

L'article du professeur Van Eck a causé, selon Schwartau beaucoup de consternation à la National Security Agency (N.S.A) et probablement aussi chez son petit frère au Canada, le Centre de sécurité des télécommunications (C.S.T.), qui sont au courant depuis plusieurs années des problèmes de sécurité reliés à ce phénomène (Programme Tempest).

La politique de sécurité du gouvernement fédéral[28] traite de ce sujet, aux pages 22 à 24 du chapitre 2.3. qui concerne les normes de sécurité relatives aux technologies de l'information. Je n'ai cependant rien trouvé de tel ni dans la Directive du Conseil du trésor du gouvernement du Québec concernant la sécurité de l'information électronique[29] ni dans le Guide de gestion de la sécurité[30], mais pour en avoir discuté avec M. Robert Cusson, je sais que les gens du Conseil du trésor sont sensibilisés à cette question.

Sans entrer dans les détails, je vais cependant mentionner trois(3) choses qui me semblent importantes:

1- L'interception des ondes électromagnétiques à l'aide du procédé découvert par le

professeur Van Eck est une arme formidable et peu dispendieuse entre les mains des guerriers de l'information;

2- Cette interception peut être faite également, semble-t-il, à partir de tuyaux, de fils électriques et de systèmes d'extincteurs d'incendie et de tout ce qui est susceptible de conduire le courant électrique. Le clavier d'un ordinateur émet aussi des signaux électromatiques lorsque vous enfoncez les touches. Ces signaux peuvent être interceptés de la même façon que ceux émis par les écrans.

3- Le ministère du Conseil exécutif et le Conseil du Trésor sont le cerveau du gouvernement du Québec. Leurs bureaux sont situés dans un immeuble commun, que l'on désigne comme le complexe "H". Si aucune mesure de protection Tempest ou autres concernant le phénomène susmentionné n'est installée à cet endroit, tous les signaux électromagnétiques émis par les écrans d'ordinateurs, les photocopieurs, les imprimantes et les télécopieurs de cet édifice peuvent être interceptés facilement dans un rayon d'un kilomètre, soit par des individus ou par des organisations. Dans un contexte controversé et tendu d'accession à la souveraineté, il y a de quoi s'inquiéter lorsque l'on sait maintenant que le Centre de sécurité des télécommunications du gouvernement fédéral a procédé, selon l'ex-agent Mike Frost[31], à l'écoute diplomatique sur une grande échelle et que leur priorité est d'empêcher la souveraineté du Québec. Le C.S.T. fait partie du ministère de la Défense Nationale. Or ce ministère possède deux (2) bâtiments situés à quelques centaines de pieds derrière le complexe "G", soit le manège militaire et une base navale appellée: HMCS Montcalm. Allez faire un tour dans ce coin-là pour comprendre ce que je veux dire.

Et, sans avoir poussé plus loin la question, je ne suis pas convaincu à priori que le Code criminel constitue une protection efficace contre ce genre d'interception.

2.5.4 - La cryptographie

La cryptographie est définie comme "la discipline qui traite des principes, des moyens et des méthodes permettant de rendre des renseignements inintelligibles et de reconvertir des renseignements inintelligibles en renseignements cohérents". Le cryptage est "la transformation de données intelligibles en une suite de caractères incohérents au moyen d'un procédé de codage réversible".[32]

Percer les codes ennemis et protéger les siens ont toujours fait partie de l'art de la guerre et de la stratégie militaire. Qu'il suffise de mentionner que les Alliés ont gagné la Seconde Guerre mondiale en partie parce qu'ils ont été capable de déchiffrer les codes allemands et japonais.

La cryptographie est avec la technologie nucléaire les deux (2) secrets les mieux gardés des gouvernements. Les États s'en servent non seulement pour protéger leurs secrets mais également pour empêcher les autres d'en avoir. Dans l'âge de l'information, tout est remis en question. Et voici pourquoi.

En **1976**, les Etats-Unis ont adopté le système Data Encryption Standard (D.E.S.), approuvé entre autres, par le Département du Trésor et qui sert à protéger les centaines de milliards de dollars digitaux qui circulent aux États-Unis chaque année. Cette technologie est protégée par une loi qui empêche son exportation en dehors des États-Unis.

Selon Schwartau, en mars et en août **1993**, deux (2) spécialistes, le premier américain et le deuxième canadien ont démontré qu'il était possible de percer le procédé en 3.5 heures à l'aide d'une superordinateur coûtant environ 1 million$.

Pour les guerriers de l'information, ce fut une bonne nouvelle. Qui n'investirait pas un

million$ pour intercepter et modifier des opérations financières importantes?

Le gouvernement américain a réagi en présentant le projet Clipper[33]. Clipper est une puce d'ordinateur qui contient un procédé d'encodage de la voix digitale et des données de communications appelé "Skipjack" et qui est destinée aux téléphones, aux télécopieurs et aux modems.

Clipper qui utilise la norme E.E.S. (Escrowed Encryption Standard), contient une "porte" (en anglais "trap door") que le gouvernement américain veut ouvrir pour effectuer la surveillance électronique sur toute pièce d'équipement qui contient cette puce. La "clef" pour ouvrir cette porte est divisée en deux (2) parties, dont l'une serait gardée par le Département du Trésor et l'autre par le département du Commerce.

Sur autorisation judicaire, les agences d'application de la loi, pourraient avoir accès aux deux (2) clefs. Pour rendre le projet applicable, le gouvernement américain a adopté une loi appelée en anglais le "Digital Telephony Bill" qui forcent les producteurs de matériel électronique à inclure la puce Clipper dans leur matériel.

Le problème, c'est qu'un représentant de la compagne AT&T a annoncé récemment que le code de Clipper pouvait être brisé. Pendant que la NSA cherche un autre code, les opposants au projet de loi - une coalition formée des libertaires du réseau Internet groupés autour de la Electronic Frontier Foundation (EFF) et de certains républicains comme Newt Gingrich, le leader du Congrès, encouragent les citoyens à utiliser les méthodes d'encryptage à clefs publiques, comme le procédé Rivest-Shamir-Adleman (RSA) ou encore P.G.P. (Pretty Good Privacy) de Philip Zimmermann qui a rendu disponible gratuitement son procédé sur le réseau Internet. Cette technique permet d'envoyer un message de façon fiable à quelqu'un sans avoir eu à échanger une clé secrète précédemment. La "signature électronique" et le "résumé de message" rendent possible l'authentification du message et garantissent qu'il n'a pas été modifié en cours de route.

Pour l'instant, le réseau Internet n'est pas visé par le Digital Telephony Bill mais la partie est loin d'être terminée. Elle met aux prises, d'une part, ceux qui se méfient en général des gouvernements et d'autre part, ceux qui insistent pour que le gouvernement puisse se réserver le droit de policer Cyberspace. Qui l'emportera?

Le problème n'est pas simple car à priori tout citoyen a le droit de protéger sa vie privée. Lorsqu'il envoie un message électronique il devrait s'attendre normalement à ce que ce message soit privé et ne soit pas intercepté par tout un chacun. S'il veut faire des achats électroniques, il doit s'assurer non seulement que son numéro de carte de crédit ne soit pas intercepté, mais également que son interlocuteur soit bien celui à qui il pense s'adresser. Tout cela exige la cryptographie.

Pour que Cyberspace se développe, il est évident que les citoyens devront utiliser le chiffrement de leurs données et il faut que cela se fasse avec des interfaces les plus conviviables possibles. PGP, à titre d'exemple, n'existe pas encore en version Windows et peut s'avérer difficile à utiliser pour les non initiés.

Par contre, il est évident qu'un puissant procédé de cryptographie utilisé par les guerriers de l'information devient une arme extrêmement importante entre leurs mains, puisqu'il sera impossible pour les gouvernements d'intercepter leurs communications et de faire appliquer leurs lois afin de se protéger et protéger leurs citoyens. Le débat est à suivre et il nous concerne tous.

A l'heure actuelle, la situation se présente comme suit: en France, la **Loi 90-1170 du 29 décembre 1970** soumet l'utilisation de toute technique de chiffrement à une autorisation, délivrée par un service qui dépend directement du Premier Ministre.[34]

Au Canada, [35] l'usage de la cryptographie n'est pas interdite sur le réseau Internet. Selon certains, il est à craindre toutefois que si les États-Unis décident de faire appliquer le "Digital Telephony Bill" au réseau Internet, le Canada suivra.

Aux États-Unis, comme je l'ai mentionné, la bataille fait rage entre l'administration Clinton et les groupes de libertés civiles comme l'Electronic Frontier Foundation[36], qui a souligné récemment que le gouvernement n'avait pas abandonné son idée d'imposer la technologie Clipper aux ordinateurs et de bannir la cryptologie forte à clef publique comme PGP. Toutefois, comme le mentionne la revue Time[37], les citoyens qui voient leur vie privée de plus en plus menacée par l'informatisation rapide de la société ont tendance à considérer cet instrument technologique moderne comme un rempart à leur liberté. A suivre...

2.5.5 - Le chipping

Le "chipping" est défini comme la modification, l'altération, la conception ou l'utilisation de circuits intégrés d'un ordinateur ou d'un système informatique pour des buts autres que ceux pour lesquels ils ont été conçus.

Le "chipping" c'est l'équivalent d'un micro (en anglais "bug") installé clandestinement dans un ordinateur ou dans un réseau informatique local.

C'est un "Cheval de Troie" électronique qui permet non seulement de capter les ondes électromagnétiques d'un système donné mais également de faciliter leur transmission à des distances considérables.

Schwartau donne l'exemple de la Corée du Nord dont les ordinateurs IBM 360 qui contrôlent leurs missiles seraient envahi par une petite puce électronique (en anglais "back door") à laquelle aurait accès le Pentagone.

Lorsqu'on la compare aux coûts exhorbitants des satellites, des sous-marins atomiques et des bombardiers B-2, le chipping est une aubaine, car il s'agit d'une arme efficace, furtive et peu coûteuse.

Mais c'est également une arme redoutable si elle tombe entre les mains des guerriers de l'information qui peuvent l'utiliser à bon escient dans toutes sortes de circonstances et contre toutes sortes de cibles, que ce soit leurs compétiteurs, les institutions financières et les gouvernements.

2.5.6. - Fusils magnétiques et autres bombes

On les appelle en anglais les HERF GUNS pour "High Energy Radio Frequency" et les EMP/T BOMBS pour "ElectroMagnetic Pulse Tranformer".

Essentiellement, un "HERF GUN" envoie un signal radio à haute puissance en direction d'une cible électronique et la met hors de contrôle. Selon Schwartau, ce genre d'arme, qui est ni plus ni moins qu'un émetteur radio, peut paralyser facilement un ordinateur et causer des dommages considérables à un réseau local ou aux commutateurs téléphoniques.

Les "EMP/T BOMBS" sont, selon Schwartau, de la même nature que les "HERF GUNS", mais mille fois plus puissants.

Selon lui, les signaux électromagnétiques catapultés à la vitesse de la lumière par cette arme électronique sont tellement puissants que n'importe quel ordinateur qui se trouve sur leur passage est détruit à jamais. Non seulement les puces de cet ordinateur sont détruites, mais également toutes les données stockées sur les disquettes, les disques durs et les bandes magnétiques.

Schwartau souligne que ces armes font partie de la panoplie des armes non létales développées par le Pentagone,[38] qu'elles sont portables et facilement fabriquables de manière artisanale ou disponibles tout simplement sur le marché.

2.5.7. - Conclusion

En guise de conclusion, qu'il suffise de mentionner que le guerrier de l'information, le moindrement habile et obstiné a à sa disposition un arsenal complet d'armes furtives, silencieuses, opérant à distance et terriblement efficaces. Vu dans cette perspective, les pays occidentaux à haute technologie apparaissent comme des colosses aux pieds d'argile, leurs pieds d'argile étant bien sûr les systèmes avancés de technologie de l'information qui leur procurent précisément un avantage majeur sur les autres pays de la planète. C'est le paradoxe de Cyberspace: ce qui fait notre force constitue également notre faiblesse.

Après avoir beaucoup parlé des armes, parlons maintenant des guerriers. Qui sont-ils?

2.6. - Les guerriers de l'information

2.6.1 - Les premiers guerriers: les "hackers" américains

Quand on pénètre dans Cyberspace, un des tous premiers mots que l'on apprend, c'est bien le terme "hacker", qui se traduit en français par le mot "pirate". La revue Time leur rend hommage dans son numéro spécial du printemps 1995. Dans un article intitulé: "We owe it all to the hippies"[39] (en francais "Nous devons cela (Cyperspace) aux hippies", le journaliste Stuart Brand écrit: "Oubliez les manifestations contre la guerre, Woodstock et même les cheveux longs. Le vrai héritage de la génération des années 1960 est la révolution informatique".

Brand définit quatre (4) périodes: la première génération de hackers a émergé à la fin des années 60 et au début des années 70, dans les départements de sciences informatiques, en imposant le "time sharing" pour rendre les ordinateurs centraux disponibles à tout le monde; une deuxième génération fin 70 a suivi qui a inventé l'ordinateur personnel. On pense à Steve Jobs, un hippie aux cheveux longs, à Steve Wozniak et à Lee Felsenstein, qui a imaginé le premier ordinateur portable.

La troisième génération a créé dans les années 80 les logiciels pour les ordinateurs personnels. On pense à Mitch Kapor, une ancien professeur de méditation transcendantale, qui a créé Lotus 1, 2, 3 et qui est le président fondateur de l'Electronic Frontier Foundation.

Enfin, la quatrième et actuelle génération des années 1990 a créé les babillards et les conférences électroniques et transformé le réseau militaire Arpanet en un réseau civil international formé de réseaux locaux et nationaux que tout le monde connaît maintenant sous le nom d'Internet, qui connaît une expansion fulgurante et irréversible.

A l'origine des hackers, il y a une philosophie et une éthique particulière que la revue française Actuel attribue - croyez-le ou non - à des Québécois, ceux de la revue Mainmise des années 1970. Dans un article intitulé: "Hackers: Quand le pavillon noir flotte sur l'ordinateur",[40], le journaliste Patrick Rambaud écrit en effet ce qui suit:

> *Les boucaniers ressemblent aux freaks de Mainmise, cette revue underground du Québec, au début des années soixante-dix. Ceux-ci combattaient un autre monopole, celui des idées assises et d'une vie trop structurée. Ils voulaient une société alternative, partaient en fourgonnette explorer l'Amérique, "pour voyager dans l'espace d'un continent troué ça et là, dans chaque région, par l'oasis d'une base de ravitaillement et de séjour".Dans le no2 de Mainmise, en mars 1972, ils prônent une électronique populaire, et la contre-culture s'établit contre ce monopole du savoir et de la surveillance qui se met alors en place, Ils réclament l'accès de tout individu à toute l'information et un ordinateur municipal à Montréal (le premier Free Net?): grâce à la machine, écrivent-ils, 90% du travail pourrait s'effectuer chez soi, les immeubles commerciaux disparaitraient du centre ville, le trafic se serait amélioré, la spéculation immobilière freinée, la surpopulation régresserait. L'Administration se cantonnerait à des tâches de gestion et d'animation, et non plus un intrument de pouvoir et de contrôle. Le citoyen pourrait, en outre, vérifier l'utilisation des budgets publics.*

Quoi qu'il en soit, armés ou non de cette philosophie libertaire et anarchiste, les hackers s'en sont donnés à coeur joie: ils se sont d'abord attaqué au téléphone (en anglais "phone phreaking") jouant comme des virtuoses au niveau national et international, juste pour le plaisir.

Puis avec l'arrivée du modem, leur intérêt s'est déplacé vers les systèmes informatiques locaux, ciblant comme le Capitaine Zap (Ian Murphy) les ordinateurs du Pentagone et de la Maison Blanche.

En **1987**, ils répandent les virus informatiques.

En **1990**, c'est l'explosion des babillards électroniques et des groupes aux noms plus bizarres les uns que les autres: Legion of Doom, Masters of Destruction, Lords of Chaos, Bas Ass

Mf, Chaos Computer Club, etc. Leurs spécialités:

- l'interception des conversations téléphoniques à partir des commutateurs publics;
- L'interception des transmissions de données;
- Le vol et la vente de mots de passe;
- Le vol et la vente de dossiers de crédit;
- La reprogrammation des commutateurs informatisés des compagnies de téléphone
- La destruction des systèmes informatiques etc,.

Quelques noms célèbres: Phiber Optix alias Mark Abene, Eric Bloodaxe alias Chris Goggans et le dernier en liste, Kevin Mitnick, arrêté en février 1992[41].

Qu'on soit d'accord ou non avec leur philosophie, il y a beaucoup à apprendre des hackers. La police l'a d'ailleurs très bien compris puisque le F.B.I. a eu recours à un hacker, Justin Tanner Petersen, pour tenter de mettre le grappin sur Kevin Mitnick.[42]

Il y aurait beaucoup à dire sur les hackers mais le temps me presse. Pour ceux que cela intéresse et comme je l'ai mentionné, il y a beaucoup de sites opérés par des hackers sur le réseau Internet. Ceux et celles qui s'occupent de sécurité informatique ont tout intérêt à visiter ces sites. Je vous en donne un qui, à mon avis, est le meilleur de tous: il s'appelle "No more secrets" et son adresse est: <http://underground.org/>. Vous trouverez à cet endroit non seulement des centaines de fichiers qui traitent de tous les trucs utilisés par les hackers au cours des ans mais aussi des logiciels de sécurité hyperperformants, comme le fameux SATAN pour UNIX qui trouve les trous de sécurité de n'importe quel système informatique

Ceci étant dit, ce serait une erreur grossière de croire que les seules menaces à la sécurité proviennent des hackers. Les vraies menaces viennent de gens qui ne sont pas nécessairement animés par une philosophie libertaire ou anarchiste ou qui sont en guerre contre l'État, mais qui sont tout simplement attirés par l'appât du gain et des intérêts économiques et financiers.

Qui sont - à part les hackers - les vrais guerriers de l'information?

Je vais me servir de la liste dressée par Schwartau puis je vais commenter brièvement s'il y a lieu:

1 - Les employés du secteur privé

Aux USA, les exemples pleuvent à la tonne d'employés du secteur privé qui commettent des infractions informatiques tout simplement par appât du gain et aucune compagnie n'est n'épargnée. Tout ce qui a une valeur: noms, adresses, dossiers de crédits, mots de passe, numéros de carte de crédit, secrets industriels, scientifiques, technologiques et commerciaux, transfert de fonds, numéros de téléphone confidentiels, etc. peut faire l'objet d'une attaque interne.

2 - Les vendeurs et les consultants

Les vendeurs de matériel électronique et informatique et de services ainsi que les consultants sont très bien placés pour mettre hors d'usage les systèmes sur lesquels ils ont contracté ou travaillé, particulièrement lorsqu'il y a des contentieux commerciaux qui les opposent à leurs cocontractants.

3 - Les fonctionnaires de l'État

Je n'apprendrai rien à personne en vous disant que les gouvernements et les États en général sont les premiers producteurs d'informations et de renseignements confidentiels ou secrets. Le gouvernement du Québec n'échappe évidement pas à la règle et il détient - entre autres - des millions de renseignements personnels sur les citoyens et citoyennes habitant son territoire. Ces renseignements valent beaucoup d'argent pour quiconque sait les utiliser intelligemment. Quand on sait que le gouvernement du Québec n'a pas de politique de filtrage sécuritaire de ses employés - comme le gouvernement fédéral, il y a de quoi s'inquiéter.

Mais ce n'est pas tout. Dans un contexte d'accession à la souveraineté et comme le passé est garant de l'avenir, j'ai des motifs raisonnables et probables de croire - pour employer une expression juridique - que le gouvernement peut être l'objet d'espionnage pour contrecarrer ses plans d'indépendance nationale. Ce serait naif et idiot de croire le contraire. Et ces attaques ne viennent pas ou ne viendront pas nécessairement de l'extérieur.

4 - Les agences d'application de la loi

Avec respect pour les policiers honnêtes, il faut être naif pour croire que les agences d'application de la loi chargées de nous protéger n'enfeignent jamais la loi. On n'a qu'à penser au Canada, aux activités illégales du Service de Sécurité de la Gendarmerie Royale du Canada qui a donné naissance à la commission MacDonald au début des années **1980**.

Aux États-Unis, selon Schwartau, le service de police de Los Angeles a violé la loi pendant une période de 50 ans, accumulant illégalement des milliers de dossiers personnels sur des politiciens, des syndicalistes, des acteurs et actrices d'Hollywood, des athlètes professionnels et des journalistes, en ayant recours à l'écoute électronique illégale.

Selon Schwartau, lorsqu'on ne parvient pas à obtenir un mandat de perquisition par la voie légale, on procède à l'écoute illégale, on va chercher des preuves et on les attribue à un informateur anonyme pour obtenir ensuite le mandat.

Comme membre du Barreau, je n'insisterai pas plus qu'il faut mais je me contenterai de souligner que ces propos sont fort pertinents, particulièrement dans le cadre de la "guerre à la drogue" où on observe le plus de violations des libertés individuelles.

5 - Les narcoterroristes

La "Guerre à la drogue" - que moi j'appelle la Grande Prohibition - est une véritable mine

d'or pour les délinquants de tout acabit. Jamais dans l'histoire de l'humanité, les organisations criminelles et les mafias de toutes sortes n'ont eu autant d'argent et de moyens que maintenant, gracieuseté des Etats prohibitionnistes.[43]

Avec l'argent dont ils disposent, il est logique de croire que ces groupes possèdent maintenant la technologie morderne pour faire trembler les états. Ils constituent déjà et ils constitueront de plus en plus dans l'avenir des redoutables guerriers de l'information.

6 - Les petits criminels et le crime organisé

J'ai toujours pensé que lorsque l'argent de papier disparaîtra définitivement pour céder sa place à l'argent digital, cela n'empêchera pas les voleurs et le crime organisé en général d'aller chercher l'argent là où il se trouvera, c'est-à-dire dans les systèmes informatiques. Le revolver et le pic du cambrioleur seront remplacés alors par le clavier d'ordinateur. Les cibles: les guichets automatiques (en anglais "Automatic Teller Machine" ou ATM) et évidemment les banques en général.

Et je ne suis pas sûr que les forces policières soient prêtes actuellement pour faire face à cette menace.

7 - Les "mailers" et les "telemarketers"

Je m'en excuse mais je n'ai pas trouvé de traduction française adéquate pour ces termes. Les "mailers" et les "telemarketers" sont ceux qui se spécialisent dans la collection de listes de noms à des fins de sollicitation postale, téléphonique ou médiatique en général. Vous n'avez qu'à penser à tout le matériel publicitaire que vous recevez par la poste et que les Américains appellent "junk mail". Vous vous êtes vous déjà demandé comment votre nom et votre adresse a été inscrit sur ces listes?

Une fois que votre nom est sur la liste, vous avez des chances d'y être pour longtemps et celui-ci se promènera, avec votre adresse, vos habitudes de consommation et vos capacités de crédit, d'ordinateur en ordinateur, de commerce en commerce et de catalogues en catalogues.

8 - Les médecins, les hôpitaux et les compagnies d'assurance

Avez-vous déjà pensé que les informations contenues dans votre dossier médical pourraient être un jour étalées sur la place publique dans le seul but de vous nuire, surtout si vous songez à vous présenter en politique. C'est pourtant ce qui est arrivé à un représentant républicain nommé Tommy Robinson qui se présentait pour le poste de gouverneur de l'Arkansas. Pendant sa campagne électorale, un article d'un journal soulignait qu'il buvait une bouteille de bourbon par jour et cette information erronée provenait de son dossier médical qui avait été falsifié.

D'autre part, les compagnies d'assurance sont des grosses consommatrices de dossiers médicaux et souvent les renseignements qui y sont contenus sont déterminants sur leur décision de payer ou de ne pas payer. Il y a beaucoup d'argent en jeu et les informations contenues dans les dossiers médicaux valent de l'or. Tout cela constitue un attrait considérable pour les guerriers de l'information.

9 - Les agences d'investigation et de sécurité privées.

Schwartau affirme que beaucoup d'agences d'investigation et de sécurité privées sont dirigées par d'anciens policiers qui sont payés pour obtenir des informations confidentielles. Or, dit-il, les informations dont leurs clients ont besoin sont souvent détenues par des organismes dont la sécurité est assurée par...d'anciens policiers. Selon lui, la solidarité qui unit la grande confrérie des policiers et des ex-policiers joue alors à plein et ces derniers peuvent se procurer les précieux renseignements qui sont interdits aux citoyens ordinaires. A-t-on des raisons de penser qu'au Québec, les choses se passent différement?

10 - Les supermarchés

Avec les moyens technologiques modernes, chaque achat que vous faites dans les supermarchés est surveillé, enregistré, stocké, comparé et analysé par des centaines d'ordinateurs. Les résultats sont souvent vendus à des firmes de marketing qui ont des catalogues personnalisés spécialement pour vous.

Imaginez ce qui peut vous arriver si vous avez le malheur comme homme ou femme mariée d'acheter des condoms avec votre carte de crédit!

11 - Les politiciens

Ceux qu'on a appelé les "plombiers du Watergate" et leurs dirigeants à la Maison Blanche étaient des guerriers de l'information. En France, la récente mise-à-jour d'une cellule d'écoute électronique au Palais de l'Élysée fait suite à plusieurs écoutes illégales qui ont eu lieu entre 1985 et 1994 visant diverses personnes, dont un journaliste, Edwy Plenel, un avocat Antoine Comte, une actrice Carole Bouquet et un écrivain Jean-Edern Halier, dont les seuls torts étaient de déplaire au gouvernement[44].

Au Canada, le premier ministre du Canada lui-même, M. Pierre Elliott-Trudeau, a été dans les années 70 un guerrier de l'information important lorsque, dans un Memorandum daté du 17 décembre 1969[45], il a exigé -et je cite - :

> *That the R.C.M. Police be asked to provide a detailed report on the present state of separatism in Quebec in terms of organization, numbers involved, organizational interrelationships, apparent strategy and tactics and outside influence.*

On connaît la suite: entre **1970** et **1975**, la GRC s'est livrée sur le territoire québécois à une soixantaine d'opérations illégales, dont le vol des listes de membres du Parti québécois en

1973. La commission MacDonald, formée de sympathisants libéraux notoires, a blanchi Trudeau et les membres de son cabinet, mais assez curieusement n'a jamais discuté du fameux Memorandum, auquel j'ai eu accès en 1992.

Il faut s'inquiéter également lorsque l'on sait maintenant, comme je l'ai mentionné, que le Centre de sécurité des télécommunications du ministère de la Défense du Canada s'est livré depuis 1973 à l'écoute électronique à partir de certaines ambassades canadiennes et que sa priorité serait, selon Mike Frost, la lutte contre la souveraineté du Québec.

12 - Les groupes d'action politique

Beaucoup de groupes politiques comme les Néo-Nazis et ceux qui prônent la suprématie de la race blanche ont le potentiel pour devenir des guerriers de l'information et certains ont déjà commencé à utiliser l'Internet pour diffuser leur propagande haineuse. Il est fort à parier que la prochaine étape les amènera tout naturellement à utiliser Cyberspace pour déstabiliser les Etats et gouvernements.

13 - Les mercenaires, les pigistes et les experts de l'ex-Bloc soviétique

Avec la chute du Mur de Berlin, il y a beaucoup de membres de services de renseignements comme le KGB et la Stasi (Allemagne de l'Est) qui ont perdu leur emploi. Ces gens ont beaucoup d'expérience dans beaucoup de domaines, du chantage et l'intimidation en passant par la désinformation jusqu'à la surveillance électronique. A qui vendront-ils désormais leurs services?

14 - Les terroristes

La bombe qui a explosé le 26 février 1993 au World Trade Center à NewYork, a fait six (6) morts et plus d'un millier de blessés, mais, comme le mentionnent les époux Toffler dans "Guerre et Contre-Guerre"[46] si les terroristes avaient lançé une attaque sur Wall Street en ciblant les réseaux

de virements bancaires, du marché des actions et des obligations, de la Bourse des marchandises, les réseaux de cartes de crédit, les lignes de téléphones et de transmission de données, les machines Quotron et les communications générales, cela aurait provoqué une onde de choc à travers le monde.

La vérité c'est qu'aujourd'hui, au moment où on se parle, un terroriste ou un groupe d'extrémistes équipés d'ordinateurs peuvent faire beaucoup plus de dégâts que la bombe du World Trade Center.

15 - L'espionnage dit "industriel"

Je n'aime pas l'expression "espionnage industriel" car le mot "industrie" est un concept d'une époque révolue ou sur le point de l'être. Je préfère parler de guerre de l'information dirigée contre des compétiteurs dans n'importe quel créneau de l'activité économique.

Je vous renvoie à ce sujet au livre de Peter Schweizer, intitulé "Friendly Spies"[47] qui analyse en détail comment les Français, les Allemands, les Israéliens, les Coréens, les Japonais, les Anglais et même les Canadiens ont espionné les corporations américaines pour soutirer des renseignements commerciaux qui leur permettaient d'obtenir une position concurrentielle favorable face aux entreprises américaines.

Qu'il suffise de mentionner que cette guerre de l'information existe tant sur le marché domestique intérieur que sur le marché international et qu'elle met aux prises des corporations entre elles et des pays entre eux. Les Américains accusent les Francais d'avoir pratiqué l'espionnage économique contre eux, mais les récents événements concernant les activités de la C.I.A. en France semblent démontrer que les Américains se sont lancés eux aussi dans cette aventure.

2.7 - Les trois (3) niveaux de guerre

Selon Schwartau, il y a trois (3) niveaux dans la guerre de l'information: le premier niveau concerne les individus, le deuxième les organisations, plus particulièrement les corporations privées, et le troisième concerne les pays.

2.7.1 - La guerre de premier niveau: les attaques contre la vie privée

Premier principe: pour les citoyens ordinaires, il n'y pas de vie privée possible dans Cyberspace à moins de prendre les moyens pour se protéger;

Deuxième principe: dans Cyberspace, il y a présomption de culpabilité car c'est l'ordinateur qui a raison à priori. Si votre dossier de crédit ou votre dossier médical contient des informations erronnées, vous pouvez avoir de sérieux problèmes;

Troisième principe: l'information est une arme qui peut être ulitisée contre vous.

Je n'ai pas à vous convaincre que les ordinateurs contiennent des millions de renseignements personnels sur la vie privée des gens et que l'interconnexion soudaine et masssive de ces ordinateurs constitue une menace sérieuse et dangeureuse à la liberté. L'assemblage des renseignements personnels contenus dans les banques de données publiques et privées peut permettre de dresser des portraits intimes extrêmement précis de nous tous et nous n'avons comme citoyens, absoluement aucun contrôle sur le contenu, son exactitude, sa dissémination ou son

usage.

La vente et le maquillage des informations, le chantage, l'extorsion, les fausses accusations et la désinformation en général sont des pratiques susceptibles de connaître une expansion fulgurante dans l'avenir, si nous ne prenons pas des mesures efficaces pour nous protéger.

Et nous ne pouvons absolument pas nous fier à la protection offerte par les lois internes sur la protection des renseignements personnels, lorsque nous savons maintenant que les attaques électroniques sont furtives, silencieuses, difficilement décelables et surtout qu'elles peuvent provenir de l'extérieur du Québec ou du Canada.

D'autre part, il faut également comprendre que les lois québécoise et canadienne sur la protection des renseignements personnels et sur l'accès à l'information datent des années 1980 et avec l'arrivée soudaine de l'Age de l'information, elles nécessisteraient à mon humble avis un sérieux dépoussiérage afin de les adapter à un nouvel environnement, que nul ne pouvait prévoir.

2.7.2 - La guerre de deuxième niveau: l'espionnage contre les organisations.

Comme le temps nous presse, je n'insisterai pas trop sur cette section d'autant plus que j'ai déjà abordé le sujet précédemment. Je contenterai de souligner cependant ce qui suit:

1- Il est à craindre que plus la compétition économique internationale augmentera, plus l'espionnage industriel et économique augmentera: en effet, selon une logique d'une désarmante simplicité, il est souvent moins coûteux et plus facile de se procurer illégalement une technologie nouvelle ou une invention que d'investir des sommes considérables en recherches et développement.

2- Dans les domaines économique, bancaire et financier, les informations privilégiées obtenues avant qu'elles ne soient rendues publiques, valent souvent des fortunes colossales réalisées en des temps records.

3- Tous les pays sont dans la course et comme le mentionne Schwartau, l'espionnage industriel et économique est devenu un passe-temps national.

4- Le vol des secrets économiques et commerciaux n'est qu'une partie des activités des guerriers de l'information: la désinformation, le chantage et la destruction des systèmes informatiques font aussi partie de leur arsenal et peuvent s'avérer très efficace pour se débarrasser d'un concurrent gênant.

2.7.3 - La guerre de troisième niveau: un "Pearl Harbor électronique"

Comme je l'ai mentionné précédemment, certains spécialistes en sécurité informatique aux États-Unis commencent à redouter une attaque massive et concertée contre leurs réseaux informatiques et de communications qui pourrait conduire à la paralysie complète du pays.

Schwartau démontre brillamment dans un chapitre intitulé "Global Information Warfare" comment les choses pourraient se passer.

Sans entrer dans les détails, disons simplement que son armée civile de l'information nécessisterait un investissement initial d'environ 100 millions de dollars - ce qui est peu compte tenu de l'enjeu - et comprendrait 13 groupes opérationnels, qui sont le suivants:

1- Un groupe de commandement que les militaires américains appelent le C4I, c'est-à-dire: le commandement, le contrôle, les communications, les ordinateurs (en anglais "computers") et le renseignement (en anglais "intelligence");
2- Un groupe des communications dont la tâche essentielle serait de constuire le réseau de communications de cette armée en utilisant tout simplement le réseau téléphonique actuel et une forte cryptographie;
3- Un groupe de navigateurs (en anglais "mappers") dont le rôle serait de tracer les cartes virtuelles des réseaux téléphoniques, cellulaires et par satellites, en mettant l'emphase particulièrement sur les réseaux bancaires de circulation de la monnaie digitale.
4- Un groupe de briseurs de code (en anglais "crackers") qui, une fois que les navigateurs auront terminé leur travail, s'emploieront à briser les mots de passe, à pénétrer dans les systèmes informatiques et à construire des ouvertures (en anglais "trap doors") pour les besoins futurs.
5- Un groupe de "renifleurs de réseaux" (en anglais "sniffers") qui se serviront des

informations recueillies par les navigateurs et les briseurs de code et qui se divisent eux-mêmes en trois (3) sous-groupes: un groupe affecté au réseau téléphonique (la "Switch"), un groupe qui s'occupe des réseaux privés et un groupe spécialisé dans l'installation physique de détecteurs ou d'équipement électromagnétique sur des cibles plus difficiles.

6- Un groupe de lecteurs (en anglais "readers") dont la tâche essentielle est d'intercepter les ondes électromagnétiques provenant des claviers et des écrans d'ordinateurs.

7- Un groupe de développement des logiciels dont le rôle est de créer des outils de travail pour les navigateurs et les briseurs de code: au menu: des logiciels "malicieux", des "Chevaux de Troie" (en anglais "Trojan Horses"), des "vers informatiques" (en anglais "Worms") et des virus.

8- Un groupe de taupes (en anglais "Moles") dont le rôle est essentiellement de transmettre des informations provenant de l'intérieur des cibles.

9- Un groupe d'analystes dont la fonction est d'analyser, à l'aide de programmes d'intelligence artificielle, les informations receuillies par les briseurs de code, les renifleurs de réseaux et les lecteurs afin de les transformer en renseignements utiles à la prise de décision.

10- Un groupe manufacturier dont la tâche principale est de construire l'équipement utilisé autre que les logiciels, comme par exemple les détecteurs de radiation Van Eck.

11- Un groupe de distribution des logiciels qui a pour fonction de mettre sur le marché des logiciels malicieux qui pourront en temps opportun agir comme des bombes à retardement.

12- Un groupe de tireurs (en anglais "shooters") qui constituent les troupes d'infanterie de l'armée de l'information: ce sont eux qui le jour de l'attaque massive manipuleront les fusils à haute énergie (en anglais "HERF Guns") et les bombes magnétiques (en anglais "EMP/T Bombs") qui détruiront les systèmes informatiques des cibles visées.

13- Et enfin un groupe de relations publiques dont le rôle sera de diffuser des

renseignements secrets pour discréditer les cibles choisies, de faire de la désinformation ou d'utiliser le chantage et l'extorsion à l'aide des renseignements recueillis par les autres groupes. Ce groupe coordonnera également les relations avec les médias lors de l'attaque massive.

Le jour de l'attaque (Jour "J"), l'objectif majeur sera de créer un black-out électronique à travers tous les États-Unis ou le pays visé. Les principales cibles seront évidemment la circulation de la monnaie (La Banque fédérale de Réserve, le Département du Revenu et Wall Street) mais aussi tous les moyens de communications et l'industrie des transports. Après avoir pris le contrôle, le groupe des relations publiques de l'armée de l'information annoncera au public américain que désormais rien ne sera plus pareil...

S'agit-il d'un cauchemar apocalyptique impossible ou d'une réalité présivible? A vous de juger et de poursuivre la discussion.

Ceci étant dit, j'en arrive maintenant à la conclusion finale.

III - CONCLUSION GÉNÉRALE

Il ne fait aucun doute dans mon esprit maintenant que le gouvernement du Québec n'a pas vraiment le choix: où nous entrons dans l'Age de l'information avec l'idée bien arrêtée de prendre la place qui nous revient en maitrisant les nouvelles règles du jeu qui se dessinent de plus en plus clairement, ou nous sommes condamnés à plus ou moins brève échéance à devenir une nation en décroissance constante, dépassée par la révolution technologique et complètement incapable de nous adapter à la nouvelle économie globale dont la richesse repose principalement sur la connaissance, le savoir et en bout de ligne l'information.

Pour surmonter ce défi, je suggère bien humblement que le gouvernement du Québec se dote le plus rapidement possible d'une "Politique nationale de l'information" qui reconnaîtrait officiellement le rôle primordial et stragégique de l'information dans la nouvelle économie mondiale et qui soulignerait la volonté ferme de ce gouvernement de faire du Québec à court terme une "nation intelligente" (en anglais "smart nation").

Pour y parvenir, le gouvernement du Québec devra s'appuyer sur les quatre (4) facteurs qui ont été mis de l'avant par Robert Steele et qui sont dans l'ordre:

1- l'interconnexion;
2- l'harnachement du contenu;
3- la coordination de la recherche et du développement;
4- la sécurité des systèmes informatiques et des télécommunications.

3.1 - L'interconnexion

L'objectif du gouvernement du Québec devrait être de créer une "communauté virtuelle de l'information", en encourageant par tous les moyens la mise en place d'un vaste réseau électronique réunissant les foyers, les écoles, les collèges et universités, les bibliothèques, les entreprises privées, les médias et les divers ministères et agences gouvernementales. On sait qu'actuellement deux (2) projets majeurs sont en marche: le projet UBI, piloté par Vidéotron et le projet Sirius de Bell.

Personnellement j'aurais tendance à favoriser la connectivité à partir de l'ordinateur plutôt que de la télévision à cause de ses plus grandes possibilités d'interactivité mais j'estime que dans un proche avenir les deux (2) technologies finiront par s'entremêler. Le jour n'est peut-être pas loin ou chaque foyer possèdera un ou plusieurs téléordinateurs à fonctions multiples. L'important c'est de faire en sorte que tous les citoyens et les citoyennes du Québec aient accès rapidement et à des coûts relativement bas à l'information utile à leur développement et à leur compétitivité dans leur créneau respectif. L'important c'est que les gens de ce pays cessent le plus rapidement possible d'être passif face à l'information et développent leur créativité et leurs connaissances en naviguant dans Cyberspace. L'important c'est de mettre fin le plus tôt possible à ce que j'appelle, moi, la "tyrannie des médias", où les gens sont à la merci des médias de masse (journaux, radios, télévision) pour être informés et sont l'objet de censure sans qu'ils s'en rendre compte.

Regardez la réaction de certaines personnes face à l'Internet. On n'entend et on ne voit que des dénonciations du réseau par les temps qui courent. Pourquoi? Tout simplement parce que ce réseau - qui est libre - menace le monopole des médias et leur contrôle sur les masses. Plus les sources d'informations se multiplient, plus ce contrôle cesse et plus la liberté augmente.

Le rôle de l'État est de favoriser la liberté des citoyens qui habitent sur son territoire et non pas de l'entraver. Pour ce faire, il devra laisser à l'entreprise privée le mandat de construire les autoroutes de l'information mais il devra veiller scrupuleusement à ce que le contenu ne soit pas contrôlé comme il l'a été dans l'Age industriel par les médias de masse.

3.2 - Harnacher le contenu

Je crois que c'est là où nous devons investir le plus. Chaque individu devrait être capable dès l'école secondaire et le collège de naviguer habilement dans Cyberspace et d'aller chercher l'information qu'il lui faut pour se former et devenir compétitif. Chaque organisation devrait avoir un responsable de l'information (en anglais "corporate intelligence officer") dont la fonction essentielle serait de recueuillir, d'analyser et de disséminer l'information utile à la prise de décision, à tous les niveaux de l'entreprise.

Au niveau gouvernemental, je suggère bien humblement que cette mission soit confiée au bureau du Vice-premier ministre tout comme le Vice-Président Gore est responsable aux États-Unis du développement de l'autoroute de l'information. Il devrait y avoir également dans chaque ministère et dans chaque organisme gouvernemental un responsable de l'information qui jouerait le même rôle.

Le gouvernement du Québec devrait mettre en place également le plus tôt possible une Fondation nationale de l'information et un Centre d'informations provenant de sources ouvertes (open source intelligence center) destinés à alimenter, particulièrement dans le domaine économique, des centres d'excellence dans le secteur universitaire et dans l'industrie privée.

3.3 - La coordination de la recherche et du développement

Je n'insterai pas longtemps sur cet item tellement il m'apparaît évident. Je mentionnerai tout simplement l'exemple de la Suède qui réussit parfaitement à intégrer son réseau universitaire, le gouvernement et les entreprises privées à la poursuite d'objectifs communs.

3.4. - La sécurité informatique et des télécommunications

Dans l'Age de l'information, un pays qui sera en mesure d'offrir au reste du monde un environnement sécuritaire pour la conduite des affaires courantes et du développement économique, possèdera une longueur d'avance sur les autres et attirera les sièges sociaux et les investissements étrangers. Voilà un défi intéressant pour le Québec et qui déborde largement les préoccupations immédiates du gouvernement du Québec sur la protection des renseignements qu'il détient dans ses banques de données.

J'ai parlé beaucoup de la fragilité et de la vulnérabilité des systèmes informatiques et des télécommunications mais il existe également toute une industrie qui se développe et donc l'objectif premier est de trouver des moyens de défense efficaces. Nous pourrons y parvenir si nous sommes conscients des dangers qui existent et j'ose espérer que j'ai pu y apporter ma modeste contribution.

D'autre part, si le Québec devient souverain, il aura les pleins pouvoirs pour agir. Dans le cadre du Canada actuel, la partie risque toutefois d'être plus serrée, car le Québec s'est fait arracher dernièrement les derniers pans de sa compétence en matière de télécommunications. J'ai mentionné

précédemment que la bataille entourant la cryptographie est un enjeu majeur aux États-Unis et cette bataille aura inévitablement des répercussions au Canada. Le Canada acceptera-t-il que le Québec développe et utilise une cryptographie forte sur laquelle il n'aura aucun contrôle? Poser la question c'est un peu y répondre. Je la laisse suspendue dans les airs pour votre réflexion et je vous remercie de votre attention.

(30)

1 Voir à ce sujet: A. TOFFLER, **Le choc du futur**, Denoel, Paris, 1974.

2 Philippe QUÉAU, **L'Ère Cyber**, Imagina, Institut National de l'Audiovisuel, Paris.

3 **Conférence ministérielle sur la société de l'information.** Conclusions de la Présidence, Bruxelles, 26 février 1995

4 **Miser sur le savoir, Rapport de conjoncture 1994, no 2 - Les nouvelles technologies de l'information**, Conseil de la Science et de la Technologie, Québec, 1994.

5 W. SCHWARTAU, **Information Warfare, Chaos on the Electronic Superhighway**, Thunder's Mouth Press, New-York, p. 59

6 N.MYHRVOLD, **Visions of the digital revolution**, Business Week, Special 1994 Bonus Issue, 24 janvier 1995.

7 A. et H. TOFFLER, **Les nouveaux pouvoirs**, Fayard, Paris, 1991

8 op. cit. note 4, p. 44

9 N. BECK, **La nouvelle économie**, Les Éditions Transcontinentales, Montréal, 1994, 221 pp.

10 op. cit. note 3, p.31

11 Voir à ce sujet: Robert David Steele, **Private entreprise intelligence, its potential contribution to national security**, Open Source Solutions Inc., 11005 Langton Arms Court, Oakton Virginia 22124-1807 - Octobre 1994

12 op. cit. note no 5, p. 150

13 Le mot "Cyberspace" a été inventé par un jeune américain expatrié à Vancouver durant les années 1980: William Gibson. Voir à ce sujet: **Welcome to Cyberspace**, Time Domestic, Special Isssue, Spring 1995, Volume 145, No. 12

14 Voir note no 2.

15 Open Source Solutions Inc, **OSS Notices**, 30 décembre 1994, p. 13

16 Voir à ce sujet: John F. QUINN, **Commercial Intelligence Gathering**, Fifth National OPSEC Conference "Managing Risk in the Information Age", 2-5 mai 1994.

17 op. cit., note no 9, p. 24

18 Ward ELCOCK, allocution du 28 octobre 1994 dans le cadre de la **Conférence internationale portant sur l'analyse et l'évaluation du renseignement** - Association canadienne pour l'étude de la sécurité et du renseignement - Ottawa, octobre 1994

19 Robert STEELE, **Theory and Pratice of Intelligence in the Age of Information**, Open Source Solutions, Inc., 17 septembre 1993

20 S. ASAI, **Outrunning Japan's Rivals**, Business Week, Sepcial 1994 Issue, 24 janvier 1994, p. 103

21 Peter SCHWEIZER, **Friendly Spies**, Atlantic Monthly Press, 1993

22 Robert STEELE, **The military perspective on information warfare: apocalypse now**, Open Source Solutions, Inc., 19 janvier 1995, p. 1

23 Voir note no 4.

24 op.cit. note 4, p.49

25 **Cops on the I-Way - Computers crimes are becoming more daring and imaginative**, Time Domestic, Special Issue, Spring 1995, Volume 145, No 12

26 Voir à ce sujet: **Computer World Expects Devil of a Time with Satan Program**, Los Angeles Time, 1er mars 1995, p. D1

27 Win VAN ECK, **Electromagnatic radiation from Video Display Units; An Eavesdropping Risk?**, PTT Dr. Neher Laboratories, Leidschendam, Netherlands, April 16, 1985

28 **Politique sur la sécurité**, Conseil du trésor, Ministère des Approvisionnements et Services Canada 1994, chap. 2.3, pp 22-24

29 La sécurité de l'information électronique, **Directive concernant la sécurité de l'information électronique et des**

actifs informationnels, Direction générale des technologies de l'information, Ministère des communications, 1993

30 La sécurité de l'information électronique, **Guide de gestion de la sécurité**, Le secrétariat, Conseil du trésor, mai 1994

31 Mike FROST, **Moi, Mike Frost, espion canadien**, Editions de l'Homme, Montréal, 1994.

32 op cit. no 30, chap 1-1, Appendice C, page C-4.

33 Voir à ce sujet: Steven Vaughan-Nichols, **It's Alive! Clipper's still kicking**, Internet World, Février 1995, p.62

34 Stéphane Bortzmeyer, **Pour la libéralisation du chiffrement en France**, adresse Internet: http://web.cnam.fr/Network/Crypto

35 Sylvain ANDRÉ, **Data Encryption and The Law(s) - Results**, Décembre 1994 - Newsgroups - talk.politics.crypto

36 Electronic Frontier Foundation, adresse Internet: http://www.eff.org/

37 Mike Godwin, **Keys to the Kingdom**, Time Domestic, Special Issue, Spring 1995, Volume 145, No 12

38 Voir à ce sujet: Heidi et Alvin TOFFLER, **Guerre et contre-guerre, Paris**, Fayard, pp. 178 et ss.

39 Stewart Brand, **We owe it all to the hippies**, Time Domestic, Special Issue, Spring 1995, Volume 145, No 12

40 Patrick Rambaud, **Hackers: Quand le pavillon noir flotte sur l'ordinateur**, Actuel, No 46, Octobre 1994, p 81 et ss.

41 **La plus dangeureux "pirate" de l'informatique enfin capturé**, La Presse, Montréal, Samedi 18 février 1995, p. A-12

42 Joseph C. Panettieri, **I was a hacker for the FBI**, Information Week, 13 mars 1995, p 12

43 Voir à ce sujet: Christian de Brie, **Chronique d'une guerre perdue**, Le Monde diplomatique, avril 1994

44 Stéphane Bortzmeyer, **Les écoutes téléphoniques en France**, adresse Internet - http://web.cnam.fr/Network/Crypto

45 Memorandum for the Cabinet Committee on Security and Intelligence, **Current Threats to National Order and Unity: Quebec Separatism**, Conseil du Trésor, Canada, S&I-10, 17 décembre 1969, p. 8

46 op. cit. note no 37, page 211

47 op.cit note no 21