# D'Echelon à PRISM

## L'impact des technologies de l'information sur la sécurité nationale

**Charles Saint-Prot**
*Directeur de l'Observatoire d'études géopolitiques (Paris)*

Début juin 2013, des journaux anglo-saxons, dont *Guardian* et *Washington Post*, ont révélé que, depuis plusieurs années, un service de renseignements des Etats-Unis, la *National Security Agency* espionne les agissements des étrangers sur le *web*, en accédant aux données des serveurs de neufs géants américains de l'Internet. Ce partenariat entre l'agence d'espionnage états-unienne et les entreprises du web, découvert grâce aux informations fournis par Edward Snowden, un ancien agent de la NSA, est connu sous le nom PRISM (pour *Planning tool for Ressource Integration, Synchronization, and Management)*. Après le scandale du système Echelon durant les années 1980, ce nouvel exemple d'espionnage technologique n'a suscité que de bien timides protestations des principales victimes de ce système, les pays européens, mais il vient rappeler l'importance de l'utilisation des technologies de l'information au service des politiques de puissance.

La fin de la guerre froide avec l'effondrement du bloc soviétique à la fin des années 1980 a coïncidé avec l'expansion spectaculaire du commerce des biens et des services, des échanges financiers et de la circulation de l'information grâce au développement des technologies nouvelles. Avec beaucoup de naïveté, certains ont cru voir l'avènement d'une ère nouvelle, marquée par la stabilité, la bonne entente générale et le bonheur. Bien sûr, l'accélération des échanges économiques et du développement des nouvelles technologies n'a pas conduit à ralentir la compétition entre les nations. La mondialisation qui résulte de la combinaison de la libéralisation des marchés et du progrès des technologies de l'information et de la communication (TIC, NITC *New Information and Communication Technologies*)**,** n'est pas un monde tranquille ni une sorte de sympathique village planétaire où tout le monde vivrait en harmonie. La réalité, c'est-à-dire les grandes constantes géopolitiques et stratégiques, n'a pas tardé à reprendre ses droits. Méprisant les utopies et les candeurs des idéologues, l'Histoire continue. Ainsi, l'interdépendance économique n'exclut pas la rivalité entre les nations, c'est-à-dire une concurrence internationale croissante sur le plan de l'économie, du commerce et de l'accès aux sources d'énergie. Cette concurrence est devenue un facteur majeur de tension et de conflits entre les puissances mondiales. L'ouverture des marchés et la globalisation (ou « mondialisation ») dissimulent mal la réalité de la guerre économique, avec ses

enjeux de monopole mais aussi de domination puisqu'il agit en fin de compte de politique de puissance. A vrai dire, il existe une logique de conflit, plus encore que de compétition. Mais, comme l'indique le directeur de l'Ecole de guerre économique à Paris, Christian Harbulot[1] ce conflit est largement dissimulé et les divers acteurs –Etats ou entreprises– n'en prennent pas toujours la mesure.

Or, depuis les années 80 du XX^e^ siècle, le système économique –comme d'ailleurs les systèmes administratifs des Etats ou le secteur de la défense– a de plus en plus été lié à la diffusion rapide de l'utilisation des nouvelles technologies de l'information et de la communication. La diffusion de l'utilisation des nouvelles technologies de l'information et de la communication est à la fois un résultat et une cause déterminante du processus de mondialisation qui a été caractérisé par la multiplication des échanges de marchandises, de services et de technologies. Les technologies de l'information et de la communication (TIC) est le terme générique désignant ce qui relève des biens et services issus des nouvelles technologies, développées à partir des années 1970 et surtout dans les années 1980, utilisées dans le traitement et la transmission des informations: radiodiffusion, télécommunications (satellite, câble, téléphonie mobile, réseaux de fibres optiques, système de positionnement par satellite[2]), informatique, Internet. Comme cela a toujours été le cas dans l'histoire de l'humanité, ces techniques de progrès ont considérablement facilité la vie des gens, les conditions de travail et la rapidité de l'accès aux informations, mais, en même temps, elles ont pu servir à des fins moins honorables. Science sans conscience n'est que ruine de l'âme écrivait déjà le grand auteur français du XVI^e^ siècle, Rabelais.

Le développement considérable des techniques modernes est donc une arme à double tranchant. Les technologies de l'information et de la communication, comme toute technologie, sont profondément « ambivalentes »[3] puisque leur impact peut être aussi bien positif que négatif dans la mesure où il offre désormais de vastes possibilités pour menacer la sécurité des personnes, des entreprises et des Etats. Nouvelles technologies signifient aussi nouvelles menaces. Les TIC permettent des formes de domination, de surveillance des personnes, des modèles de marketing, des stratégies de manipulation et d'influence, voire d'hégémonie. Les sociétés modernes sont de plus en plus

---

[1] HARBULOT, Christian. *La machine de guerre économique*. Paris : Economica, 1992.

Voir également : HARBULOT, Christian et BAUMARD Philippe. *La main invisible des puissances*. Paris : Ellipses, 2007 (2^e^ édition).

[2] Le principal système de positionnement par satellite est le *Global Positioning System* ou GPS.

[3] DE CERTEAU, Michel. *L'invention du quotidien*. Paris : Gallimard, 1990.

dépendantes des technologies de l'information, y compris dans leur fonctionnement quotidien. Les transactions financières et commerciales, d'une part, la production industrielle et la gestion de l'énergie, d'autre part, reposent sur ces mêmes technologies. De même, les systèmes de défense incorporent de plus en plus d'informatique. Ce rôle grandissant des technologies de l'information et de la communication a provoqué l'accroissement des vulnérabilités potentielles. La menace concerne tous les secteurs, en particulier les entreprises de haute technologie, les secteurs de la recherche, l'industrie et la fabrication, la commercialisation ou encore le secteur tertiaire.

Dans ces conditions, la nouvelle guerre pour l'information –s'inscrivant elle-même dans la guerre économique globale– est aujourd'hui une réalité indéniable dans la mesure où le pouvoir c'est l'information, sa connaissance et sa maîtrise(I). Dans ce domaine, les Etats-Unis ont pris une large avance en utilisant les nouvelles technologies de l'information au service d'une stratégique de domination économique qui se place dans une perspective hégémonique globale. A cet égard, les exemples du réseau *Echelon* ou de la prépondérance sans l'Internet sont très révélateurs d'une suprématie conquérante et jalouse de ses prérogatives (II).

Les Etats et les nations doivent donc mesurer exactement l'enjeu. Il est indispensable de prendre conscience du danger pour la sécurité économique, comme d'ailleurs de la sécurité nationale dans son ensemble (politique, militaire, culturelle, etc.). Il s'agit de se prémunir et d'agir. Il est donc nécessaire que les Etats, en liaison avec les acteurs économiques, développent des stratégies d'intelligence économique adaptées à la menace et au contexte de la nouvelle guerre (III). Il est également souhaitable que la question des menaces dues aux technologies de l'information et de la communication fasse l'objet d'une régulation par un renforcement du droit international et par une gouvernance mondiale de ces technologies (IV).

## I- Guerre économique, information et TIC

L'un des pères du libéralisme économique, Adam Smith (1723-1790), prétendait que dans l'économie de marché une main invisible régule justement les échanges de façon que la libre concurrence ait une action pacificatrice et harmonieuse. Le triomphe du libéralisme après l'écoulement du bloc soviétique devait ouvrir une ère de parfaite harmonie entre les nations. La mondialisation aurait donc dû se traduire par l'instauration de la « république économique universelle » que prédisait Adam Smith. On sait que la réalité est bien différente. La règle est l'ultracompétitivité entre les nations. En outre, loin de soulever l'enthousiasme, le développement de nouvelles puissances économiques, comme la Chine ou l'Inde, est un facteur d'inquiétude pour les puissances

traditionnelles. Dans ce contexte, l'information est au centre de la guerre économique entre les Etats (1), ce qui confère une place essentielle aux technologies de l'information et de la communication (2).

## 1- Le pouvoir c'est l'information

La fin de la guerre froide a provoqué un bouleversement considérable dans la mesure où les puissances ont redéfini leurs priorités stratégiques dans le double contexte de l'accélération de la libéralisation des échanges économiques mondiaux et du développement rapide des nouvelles technologies de l'information et de la communication. L'économie a donc renforcé son rôle dans les grands enjeux géopolitiques et l'on a redécouvert que la puissance économique est, comme l'écrit William Warner[4], une composante fondamentale de la puissance nationale ("economic power is the fundamental component of national power"), c'est-à-dire que la sécurité nationale est tout aussi bien une question de vitalité économique que de seule capacités militaires. Sans sous-estimer le jeu des autres pays, force est de reconnaître que le ton est donné par les Etats-Unis qui restent la première puissance économique du monde. Dès la chute du bloc soviétique, les Etats-Unis ont redéfini une stratégie intégrale visant à leur permettre de demeurer une superpuissance et de faire prévaloir leurs intérêts économiques sur leurs concurrents européens ou asiatiques; ces deux objectifs étant intimement liés.

La géopolitique mondiale est désormais dominée par une superpuissance dont l'objectif est de maîtriser le capitalisme mondial, façonner le marché à sa convenance, s'assurer des ressources énergétiques et du des routes stratégiques de l'énergie, et, finalement, faire en sorte que la mondialisation soit une américanisation sur tous les plans[5]. Les Etats-Unis considèrent qu'il est vital pour leurs intérêts nationaux d'exercer une supériorité dans les secteurs de l'énergie, de l'aéronautique et de l'espace, de la défense et des technologies de l'information. En 1993, le président Clinton, qui venait de créer le National Economic Council, mettait en exergue la relation entre la vitalité économique et la sécurité nationale. Il exposait que la défense des intérêts économiques est devenue l'axe prioritaire de la stratégie des Etats-Unis et il donnait une dimension accrue à l'intelligence économique (*Competitive Intelligence*). Il est remarquable que la démarche américaine ait accordé une place de choix aux nouvelles technologies de l'information dans la mesure où la maîtrise de la

[4] WARNER, William T. "International Technology Transfer and Economic Espionage". *International Journal of Intelligence and Counterintelligence*, Volume 7, n° 2, Summer 1994, 143-160.

[5] Voir BRZEZINSKI, Zbigniew. *The Grand Chessboard. American Primacy and It's Geostrategic Imperatives* 1997.

connaissance est devenue un objectif prioritaire en matière économique. C'est pourquoi, l'un des aspects de la guerre économique est la guerre de l'information, laquelle est définit par le Dr John Alger, de la National Defense University à Washington, comme « l'ensemble des actions entreprises dans le but d'obtenir la supériorité de l'information, en affectant les informations, le traitement de l'information et les systèmes d'information de l'ennemi, tout en protégeant ses propres informations, traitements de l'information et systèmes d'information »[6]. La doctrine nouvelle des Etats-Unis vise « l'ensemble des actions entreprises pour atteindre la supériorité dans l'information en agissant sur l'information, « les processus informationnels, les systèmes d'information et les réseaux informatiques de l'adversaire, tout en défendant sa propre information, ses propres processus informationnels, ses systèmes d'information et réseaux informatiques »[7].

. Comme le renseignement a toujours été l'un des nerfs de la guerre classique, l'information est le nerf de la guerre économique. C'est une clé du pouvoir économico-politique Dans un environnement mondialisé et fortement concurrentiel, la maîtrise de l'information joue un rôle déterminant dans les prises de décision destinées à conquérir de nouveaux marchés, à s'approprier des sources d'énergie, à s'assurer une position privilégiée dans tous les secteurs dits stratégiques ou à obtenir renseignements ciblés sur les concurrents. Le contrôle des flux d'information mondiaux est un objectif essentiel. La maîtrise de l'information et des circuits d'information est un enjeu stratégique, c'est l'un des socles du pouvoir. Le rôle du renseignement a été considérable dans les affrontements économiques qui se sont toujours déroulés au cours de l'Histoire. Aujourd'hui, l'information est une matière première stratégique puisque l'information c'est le pouvoir. La maîtrise de l'information et la capacité à en disposer constituent des atouts essentiels de puissance. Le contrôle des sources de l'information est le but ultime d'une bataille planétaire qui ne dit pas son nom. Il s'agit pour les Etats ou les grandes multinationales d'obtenir certaines informations primordiales sur le plan économique et ainsi avoir une position des plus intéressantes sur les marchés commerciaux. Mais il est notable que l'enjeu n'est pas le savoir lui-même, mais son contrôle de son émergence à sa diffusion[8] de façon à modifier des rapports de force par l'emploi délibéré d'information visant à transformer l'évaluation d'un décideur ou d'une opinion.

---

[6] ALGER, John I. « Declaring Information War: Early Training Crucial to Awareness». *Jane's International Defense Review* 29, July 1996: 54-55.

[7] DANINOS, Frank. « Guerre et dominance informationnelle : origines, histoire et significations». *Diplomatie*, no 2, mars-avril 2003, p. 9.

[8] FRANCART, Loup. *Infosphère et intelligence stratégique: les nouveaux défis*. Paris : Economica, 2002.

L'économie mondiale n'est pas caractérisée par la concurrence libre et loyale imaginée par les penseurs libéraux des siècles passés. De fait, la concurrence est faussée par toutes sortes de procédés. L'âpreté de la compétition économique mondiale provoque une utilisation massive de l'information et de la connaissance pour déstabiliser la concurrence, pour acquérir des renseignements technologiques ou pour préserver et développer une position dominante par la désinformation, les rumeurs ou les manipulations médiatiques[9]. C'est pourquoi, les services de renseignement des grands Etats déploient une intense activité en la matière, notamment les services américains et chinois qui sont les deux géants de l'espionnage technologique.

Maîtriser l'information permet donc de faire prévaloir ses intérêts et de menacer la sécurité économique de ses concurrents ou adversaires en même temps que cela offre la possibilité d'imposer un modèle de société, de consommation, de culture, d'économie, de cadre juridique et normatif.

### 2- Le rôle des TIC

On sait depuis longtemps que la technologie est toujours un moyen de la puissance. Sa circulation, son appropriation et son partage sont donc des enjeux stratégiques permanents pour les Etats comme pour les agents économiques. La technologie a toujours été un moyen de la puissance, « sa circulation, son appropriation et son partage sont donc des enjeux stratégiques permanents pour les Etats comme pour les agents économiques »[10]. Ce qui est nouveau, c'est le développement des technologies électroniques, l'explosion de l'informatique, les progrès des techniques de traitement du signal, enfin la conquête de l'espace. Tout cela « offre des moyens considérables pour recueillir, traiter, modifier, diffuser l'information »[11].

.Les technologies de l'information et de la communication sont devenues une composante essentielle du système économique mondial. L'utilisation des réseaux électroniques a favorisé la multiplication et la promptitude des échanges, elle a stimulé la compétitivité, elle a modifié considérable les règles de la « vieille économie » et bouleversé les comportements des agents économiques, les processus de décision ou encore l'organisation des entreprises. Le marché des technologies de l'information se présente comme un vaste

---

[9] Voir « Les applications économiques de la guerre de l'information ». Site infoguerre.com Lien : www.infoguerre.com/article.php?sid=34

[10] WARUSFELD, *Bertrand.* « Nouvelles technologies et relations internationales ». *Annuaire français des relations internationales*, AFRI, vol IV, 2003.

[11] GILLYBŒUF, Jean-Paul. « La maîtrise de l'information, un enjeu stratégique ». Revue Agir, n° 25, mars 2006.

chantier ; ces technologies constituent l'un des éléments les plus dynamiques et les plus novateurs de l'économie tout en constituent un important facteur de croissance, comme l'atteste l'exemple de l'Inde qui a acquis un nouveau rang dans l'économie mondiale en partie grâce au secteur des TIC qui a connu une croissance de près 45% par an depuis 1995. En termes d'emploi, les TIC représentent des réservoirs considérables et elles confèrent à ceux qui les maitrisent une suprématie écrasante. Les grandes puissances sont donc lancées dans une intense course aux innovations technologiques parallèlement à la guerre économique à laquelle elles se livrent.

Ces innovations ne sont évidemment pas neutres et elles n'excluent pas des comportements criminels ou agressifs. François-Bernard Huyghe souligne que le développement des technologies de l'information n'a pas seulement des effets positifs, il suscite également des effets négatifs : intoxication, falsification, domination informationnelle. Ces technologies « se prêtent à des utilisations hégémoniques ou incapacitantes »[12], elles favorisent des activités illégales, clandestines ou coercitives menées par des gouvernements pour avoir accès sans autorisation à des renseignements économiques ou technologiques stratégiques. Le danger pour la sécurité nationale, dont la sécurité économique, est multiple: la guerre électronique, qui permet de dégrader, modifier, détourner les signaux et informations utilisés et transmis par les moyens de communication et les moyens de détection (radars, autodirecteur) ; L'interception de la transmission d'informations par les réseaux filaires vulnérables au niveau des routeurs et par les réseaux sans fil de type « WiFi », dont le développement présente de nouvelles vulnérabilités ; le piratage des moyens informatiques, qui, au travers d'accès illicites aux ordinateurs, par des individus maîtrisant les mécanismes de sécurité informatique (*hackers*), permet de dégrader, de modifier leur fonctionnement, voire de les neutraliser ; la destruction physique des centres de commandement et des moyens de liaison sur le terrain; les opérations psychologiques ou les campagnes de désinformation facilitées par les facilités de communication, *etc.*

L'analyse des comportements criminels *stricto sensu* n'entre pas dans le champ de cette étude qui s'intéresse plus particulièrement aux stratégiques de puissance et aux risques pour la sécurité économique des nations et de leurs entreprises. Outre le cyber-terrorisme ou la cyber-violence qui porte atteinte à la bonne santé morale des sociétés (pornographie, pédophilie, racisme, jeux débilitants ou violents), nous rappellerons simplement que les comportements délictueux utilisant les possibilités offertes par les TIC sont nombreux, notamment la criminalité informatique –souvent appelée cybercriminalité– qui peut prendre des formes très variées comme l'altération à distance d'une base de

[12] HUYGHE, François-Bernard. *L'ennemi à l'ère numérique.* Paris : PUF, 2001

données, les attaques de virus, l'envoi de, virus, de vers ou de chevaux de Troie, la prise de contrôle sur un cerveau électronique, les attaques contre les systèmes informatiques cruciaux d'un pays, d'une administration, d'une entreprise ou d'un secteur commercial pour les contrôler ou les rendre inefficients. Il est clair que cette forme de nuisance peut être purement criminelle mais peut également viser des objectifs politiques, terroristes ou économiques. Dans ce dernier cas, elle est l'un des aspects de la guerre économique ou de la lutte pour la détention de l'information. Il est vrai que dans la guerre économique tous les coups sont permis[13], comme le démontre l'exemple de la stratégie des Etats-Unis en matière de domination économique.

## II- D'Echelon à PRISM, les grandes oreilles des Etats-Unis

Pour les Etats-Unis, l'économie est donc l'un des fondements majeurs du concept de sécurité nationale qui n'est, en l'occurrence, que le synonyme de la politique d'hégémonie de l'hyperpuissance mondiale. Il est notable qu'un lien étroit relie les services de l'Etat, notamment les diverses officines de renseignement, aux entreprises américaines. Au service de cette politique, l'information joue un rôle redoutable et, dans ce domaine, les nouvelles technologies de l'information et de la communication sont largement utilisées au profit de la veille stratégique, de la surveillance concurrentielle, de l'évaluation des risques ou du repérage des avancées techniques des autres pays. Bien sûr, de nombreux pays –par exemple, la Russie, le Japon ou la Chine– n'ont pas hésité à utiliser les nouvelles technologies à des fins de renseignement économique mais aucun n'a pu mettre en œuvre autant de moyens que les Etats-Unis. C'est pourquoi l'exemple de la stratégie des Etats-Unis doit être faire l'objet d'une étude objective qui ne vise pas à faire un procès à ce grand pays mais à rendre compte d'une situation de fait.

Pour répondre tant aux défis nouveaux en matière de guerre de l'information qu'à la stratégie globale de leur nouvelle politique internationale les Etats-Unis ont déployé « un élargissement des moyens et des tactiques de renseignement »[14]. L'un des aspects significatifs de la stratégie des Etats-Unis est le système connu sous l'appellation «Echelon» (1). La maîtrise des Etats-Unis sur la gestion d'Internet doit également être soulignée (2). Par ailleurs, il est intéressant d'étudier le modèle de partenariat public-privé représenté par le fonds d'investissement de la CIA, *In-Q-Tel* qui a pour objet la veille

[13] LAÏDI, Ali. *Secrets de la guerre économique.* Paris : Seuil, 2004.

[14] DELESSE, Claude. « Le réseau Echelon et la puissance informationnelle américaine ». *Annuaire français des relations internationales*, vol. V, 2004.

technologique et commerciale stratégique tout autant que le transfert de technologies civiles (3). En tout cas, comme le montre l'affaire PRISM, les Etats-Unis ne sont pas prêts de renoncer à leur stratégie en la matière (4).

### 1- le réseau Echelon

Echelon est un système d'interception mondial des communications fonctionnant avec la participation –en fonction de leurs capacités– des Etats-Unis, du Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande. Ces pays sont liés par l'accord UKUSA (*United Kingdom - USA Security Agreement*). Signé secrètement en 1947**,** cet accord fixe les termes de la collaboration et du partage d'informations de leurs services de renseignement. A l'origine, le traité UKUSA portait sur la coopération des pays concernés dans le domaine de l'écoute électronique dans le cadre de la guerre froide qui a suivi la seconde guerre mondiale.

Le système Echelon est géré par la National Security Agency (NSA), qui en est le principal maître d'œuvre, avec la collaboration des services de renseignement des quatre autres pays impliqués, en particulier le GCHQ britannique équivalent NSA. La NSA est compétente, non seulement de tout ce qui a trait à la sécurité informatique des Etats-Unis, mais aussi pour la surveillance, de l'interception et du déchiffrement des télécommunications (téléphone, télécopies, courriels). Le système Echelon est un réseau global, appuyé par des satellites artificiels, de bases d'écoutes situées aux États-Unis, au Canada, au Royaume-Uni (notamment à Menwith Hill qui est la plus importante base du réseau et est placée sous le contrôle de la NSA), en Australie et en Nouvelle Zélande, de petites stations d'interception ; soit au total 175 stations d'interception disséminées dans plus de 50 pays, auxquelles il faut ajouter des sous-marins, en particulier le *USS Jimmy Carter,* qui écoute les câbles sous-marins de télécommunications. Il est capable d'intercepter un très grand nombre de télécommunications (téléphone, télécopies, internet…) puis d'y détecter des mots-clés grâce à un puissant réseau d'ordinateurs. Selon Nicky Hager, la clé de l'interception « repose sur de puissants ordinateurs qui scrutent et analysent ces masses de messages pour en extraire ceux qui présentent un intérêt. Les stations d'interception reçoivent les millions de messages destinés aux stations terrestres légitimes et utilisent des ordinateurs pour dénicher ceux qui contiennent des adresses ou des mots-clés préprogrammés »[15].

Le système défensif et militaire qui a intégré au fil des ans toutes les technologies nouvelles, s'est peu à peu dévoyé pour finir par être un instrument

[15] HAGER, Nicky**.** *Secret Power, New Zealand's Role in the International Spy Network*. Nelson (NZ): Craig Potton Publishing, 1996.

d'espionnage économique au service des entreprises anglo-saxonnes, en particulier des Etats-Unis. Claude Delesse note que les cibles ont évolué à travers les différentes phases du système des relations internationales : « À partir des années quatre-vingts, Echelon se focalisa sur les nouvelles menaces liées au terrorisme international. Dans les années quatre-vingt-dix, les rapports de force classiques entre Etats démocratiques se sont progressivement estompés derrière les rivalités économiques et financières, terrain de prédilection de la géo-économie. Le concept de sécurité économique privilégié par l'Administration Clinton a bien reflété ce déplacement des priorités pour les Etats-Unis. De nombreux cas d'interceptions de renseignements à des fins économiques confirment cette évolution, qui a entraîné un regain incontestable des activités de surveillance d'Echelon »[16].

C'est ainsi que la NSA retransmet les informations concernant le développement technologique, la recherche ou les activités économiques des concurrents aux entreprises par l'intermédiaire de certains organismes tel l'*Advocacy Center*, l'agence du. Département du Commerce américain de soutien au commerce extérieur qui assure la coordination des ressources de tous les organismes gouvernementaux des États-Unis pour s'assurer que les ventes des produits et des services américains puissent avoir les meilleures perspectives à l'étranger et qui de mettre au service des sociétés américaines la totalité des dispositifs publics -y compris les agences de renseignement - pour les aider face à leurs concurrents étrangers.

Initialement censé servir à l'espionnage du bloc soviétique, Echelon n'a donc pas disparu avec la fin de la guerre froide. Tout en maintenant son volet militaire et de lutte contre diverses formes de criminalités (terrorisme, trafic de drogue), il n'a fait qu'accentuer le volet d'espionnage économique. A cet égard, on peut citer, en 1990, l'interception des communications entre le fabricant japonais de satellites NEC et l'Indonésie pour la fourniture d'un contrat de 200 millions de dollars ; en 1994, le vol d'éléments techniques pour la constructions d'éoliennes à la société allemande *Enercon*, l'interception des offres de l'entreprise française Thomson CSF pour la construction d'un système de surveillance de la forêt amazonienne, l'interception des courriels des représentants européens dans le cadre des négociations sur le GATT ; en 1995, l'affaire de ventes d'avions à l'Arabie saoudite, opposant McDonnell Douglas à Airbus ou l'espionnage des cadres japonais de Toyota et Nissan lors des négociations sur les droits de douane et les quotas d'importation des voitures japonaises.

[16] DELESSE, Claude. « Le réseau Echelon et la puissance informationnelle américaine ». *Annuaire français des relations internationales*, vol. V, 2004.

Sans doute bien connu des divers services de renseignements des Etats, le réseau Echelon a été dévoilé au grand public une première fois par un journaliste écossais, Duncan Campbell, dans un article publié dans le magazine britannique *New Statesman,* le 12 août 1988[17]. Dans son article, Duncan Campbell précisait que le système Echelon rapportait, chaque année, 25 milliards de dollars de contrats aux firmes américaines. Mais ce n'est qu'en 1996, que nom d'Echelon a été connu grâce à la publication du livre du Néo-zélandais Nicky Hager : *Secret Power*[18]. En 1999, Duncan Campbell a remis au Parlement européen un rapport très détaillé sur les agissements d'Echelon et sur les dangers que faisait peser ce réseau sur les pays de l'Union et sur leurs entreprises[19]. Les Etats-Unis n'ont pas nié ces informations. ¨Plus encore, en mars 2000, James Woolsey, ancien directeur de la CIA, a publié un article dans le Wall Street Journal, intitulé « Pourquoi l'Amérique espionne ses alliés » et visant à justifier l'espionnage économique réalisé par le biais d'Echelon. Plus encore, les Etats-Unis ont profité des attentats du 11 septembre 2001 à New York et contre le Pentagone, pour accentuer le réseau Echelon sous couvert de combattre le terrorisme.

La découverte, fort tardive, d'Echelon provoqua une grande gêne dans les relations internationales. Des commissions parlementaires furent instituées dans plusieurs pays, notamment en France, et au sein du Parlement européen qui créa, en 2000, une commission temporaire « sur le système mondial d'interception des communications Echelon ». Parmi les nombreux documents de travail, cette commission a appuyé ses conclusions sur le rapport détaillé de Duncan Campbell. Le 5 septembre 2001, le Parlement européen a adopté une résolution approuvant les travaux de la commission. Le texte affirme que « l'existence d'un système d'interception mondial des communications fonctionnant avec la participation, en fonction de leurs capacités, des Etats-Unis, du Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande (…) ne fait plus de doutes », et qu' il est incontestable qu'il est utilisé « pour intercepter des communications privées et économiques, mais non militaires ». Il faudra attendre octobre 2003 pour que le Parlement de Strasbourg décide la création d'une agence de lutte contre les menaces électroniques : l'*European network and information security agency* (ENISA) Pour le reste, la réaction des Etats

---

[17] CAMPBELL, Duncan. « Somebody's listening ». *New Statesman*, 12 août 1988, p. 10-12.

[18] HAGER, Nicky**.** *Secret Power, New Zealand's Role in the International Spy Network*, ouvrage précité.

[19] CAMPBELL, Duncan. *Interception Capabilities 2000: Development of Surveillance Technology and Risk of abuse of Economic Information*.STOA, Parlement européen, PE 168 184, avril 1999. Voir le site de Duncan Campbell : www.duncan.gn.apc.org

membre de l'Union européenne est restée très timide et ils ont d'autant moins su –ou voulu- adopter une réponse appropriée qu'on voit mal comment ils pourraient un système de protection communautaire alors qu'un des membres de l'Union européenne, la Grande Bretagne, est liée aux Etats-Unis.

En tout cas, l'affaire Echelon a mis en évidence l'utilisation globale des nouvelles technologies de l'information et de la communication à des fins de renseignement économique par une puissance au détriment de la sécurité économique des autres pays. En même temps, le scandale soulevé par le système Echelon a conduit certaines puissances à renforcer ou à se doter de leur propre système d'écoute électronique spatiale. La plupart des Etats désireux de maintenir leur influence dans le monde (la Chine, la Russie, la France, l'Allemagne, Israël, l'Inde, le Pakistan, divers pays d'Asie du Sud) possèdent eux-mêmes un réseau d'écoute spécifique, intégré à leur système de défense et de renseignement, même si celui-ci ne revêt pas l'importance quantitative de celui des Etats-Unis. Outre la Russie, la France, qui est l'un des rares pays avec les Etats-Unis et leurs alliés à disposer, avec ses départements et territoires d'Outre-mer et sa présence militaire dans certaines de ses anciennes colonies, de territoires répartis dans le monde entier, a développé au cours des années 1990 un système qui a permis de mettre en place le système d'écoute électronique spatial ESSAIM dont les microsatellites ont été lancé, en 2004, par le lanceur Ariane 5 à partir de la base de Kourou en Guyane française.

### 2- La domination d'Internet

Un autre aspect du déroulement de la stratégie des Etats-Unis par l'utilisation des technologies de l'information concerne Internet. On sait que le réseau informatique mondial est né d'un programme Aparnet développé durant les années 1960 par le département américain de la Défense. Pour des raisons historiques, les Etats-Unis sont en position hégémoniques. La plupart des liaisons passent par les Etats-Unis, les systèmes d'exploitation, qui sont au cœur des systèmes d'information, sont dominés par Microsoft qui est en position de quasi-monopole et 75% des logiciels commercialisés dans le monde sont conçus aux Etats-Unis (essentiellement par Microsoft), les utilisateurs d'Internet ont recours aux navigateurs américains *Explorer* de Microsoft, *Navigator* de Netscape ou *Safari* d'Apple ; les plus importants moteurs de recherche sont également américains (Google, Yahoo) ainsi que les produits concernant les courriers électroniques, la messagerie dominée par Yahoo!, MSN (Microsoft Network), AOL (America Online) ou Skype, le système de téléphonie gratuit passant par le Réseau inventé par des Scandinaves, qui a été racheté par le site de vente aux enchères américain eBay. Certains pays prennent la mesure du danger causé par cette situation. Par exemple, en août 2004, le gouvernement chinois a décidé de travailler à la réalisation d'un système d'exploitation inspiré

du noyau de système d'exploitation libre Linux, qui serait spécialement dédié à ses propres besoins et ne serait pas menacé de contenir les «backdoors» que l'on suspecte parfois les logiciels commerciaux américains d'avoir pu installer à la demande de la NSA

Plus encore, il est constant que les services américains exercent une tutelle effective sur Internet, notamment en raison du fait que de nombreuses infrastructures se concentrent aux Etats-Unis. Le gouvernement d'Internet est assuré par des organismes publics et privés créés et contrôlés par les Etats-Unis.

Le cas le plus emblématique est celui du contrôle exercé par l'ICANN (*Internet Corporation for Assigned Names and Numbers*) qui, d'une part, par sa branche IANA (*Internet Assigned Numbers Authority*), coordonne et attribue les adresses IP (*Internet Protocol*) que doivent posséder tous les ordinateurs et, d'autre part, gère les protocoles et les noms de domaine Internet, *Domain Name System* (DNS). Le DNS est un instrument essentiel qui fournit un moyen d'appliquer des sanctions aux utilisateurs : le refus d'accès aux noms de domaine est l'équivalent du bannissement d'Internet. Les Etats-Unis sont en train de créer, avec la participation du département de la Défense et la société *VeriSign*, une nouvelle génération de DNS, qu'on ira bientôt vers l'ONS (*Object Name System*), qui s'appuiera sur les technologies du RFID (*Radio Frequency Identification*) Il s'agira d'un outil non seulement de connaissance, mais aussi de maîtrise potentielle des informations associées au commerce mondial. Tout ceci aura un impact économique considérable et pose la question de la gouvernance mondiale d'Internet. C'est pourquoi, la demande d'une régulation internationale de la mise en œuvre des technologies de l'information et de la communication s'exprime de manière croissante, aussi bien dans les pays européens qu'en Chine ou en Amérique latine.

### 3- La veille technologique

Les Etats-Unis développent également une intense veille technologique. L'un des aspects de cette veille est la création par la CIA, en 1993, d'une société de capital-risque, travaillant en liaison avec des grands organismes américains des hautes technologies : In-Q-Tel[20].

L'objectif d' In-Q-Tel consiste à détecter des technologies innovantes susceptibles d'être utilisées par les services de renseignement puis d'investir dans les sociétés les plus avancées ou les plus prometteuses dans les secteurs des nouvelles technologies permettant de collecter, d'analyser et de diffuser le

[20] La référence à " Q ", le chercheur et fournisseur de gadgets du célèbre espion de fiction James Bond*, est très révélatrice.*

renseignement. Bernard Carayon a pu noter qu'In-Q-Tel constitue un modèle de partenariat Public-Privé, il est vrai que « les besoins en technologies de l'information de la CIA sont communs de 70 à 90 % avec ceux des grandes entreprises américaines »[21].

In-Q-Tel concentre ses investissements sur des secteurs clés: le *Knowledge Management* et la représentation graphique, la recherche d'information, la sécurité et la protection, la diffusion des données, les technologies géospatiales. Le rapport Carayon précise qu'In-Q-Tel choisit « les technologies du marché, des standards garantissant la pérennité des technologies exploitées et la rentabilité des entreprises dans lesquelles sont réalisés les investissements ». Depuis le début de ses activités, In-Q-Tel a investi dans des dizaines de sociétés. Par exemple, la question du pillage technologique a été posée lorsque, en 2001-2002 , In-Q-Tel a permis à un fonds d'investissement américain, Texas Pacific Group (TPG), d'entrer à 26% dans le capital de la société française Gemplus, chef de file mondial de la carte à puces et secteur dans lequel les Etats-Unis accusent un retard. Le siège social de la société a été installé à Luxembourg et un nouveau PDG a été nommé, Alex Mandel qui est un ancien administrateur du fonds d'investissement de la CIA.

### 4- L'affaire PRISM

Un nouveau scandale révélé en juin 2013 a démontré la permanence de la politique des Etats-Unis en matière d'espionnage et de contrôle des nouvelles technologies. Grâce aux informations fournies par un ancien collaborateur de la NSA, la presse a pu mettre en lumière l'ampleur de la collecte systématiques de données privées dans les serveurs des géants du Web (Google, Apple, Facebook….) par les services de renseignements américains dans le cadre du programme PRISM (*Planning tool for Ressource Integration, Synchronization, and Management*) qui permet à la NSA de se connecter aux serveurs de neuf entreprises (Google, Yahoo!, Apple, Facebook, Youtube, Skype, Aol, Microsoft et Paltalk), via un portail, pour consulter et récolter les informations des utilisateurs. Toutes sortes de données sont ainsi récoltées : les adresses de courriels, les textes des courriels, les vidéos, les photos, les discussions privées, les documents transférés… Les informations recueillies sont analysées par un autre logiciel de la NSA, *Boundless informant*, puis stockées dans les centres de

[21] CARAYON, Bernard *Rapport d'information sur la stratégie de sécurité économique*. Paris : rapport n° 1664, Assemblée nationale, 2004.

Voir également CARAYON, Bernard. *Patriotisme économique : De la guerre à la paix économique*. Paris : Editions du Rocher, 2006.

données (*datacenters*) de l'agence. Près de cent milliards de données seraient collectées chaque mois.

PRISM a été mis en place sous la présidence de George W. Bush en 2007, afin d'intensifier la lutte anti-terroriste, ce prétexte sécuritaire étant toujours mis en avant pour toute sorte d'opérations de nature totalement étrangère à cet objet légitime. La violation du droit que constitue PRISM s'opère sans aucune ordonnance de justice mais s'appuie sur une base légale, le *Protect America Act***,** instauré en 2007 qui permet de surveiller les données virtuelles et le *FISA Amendements Act* (2008) qui garantit l'impunité aux entreprises qui coopèrent avec les autorités en leur fournissant des renseignements. PRISM s'est fortement développé sous la présidence de Barak Obama qui a mis en exergue la nécessité des collectes secrètes de données par les services de renseignement dans le cadre de la lutte antiterroriste. Ce président qui, par ailleurs, encourage une diplomatie américaine activiste utilisant le prétexte des droits de l'homme, a cru pouvoir exciper d'un « compromis » entre protection de la vie privée et les exigences de la lutte antiterroriste.

## III- L'Intelligence économique : une affaire d'Etat

Le développement conjoint de la libéralisation des échanges dans le cadre de la mondialisation et des technologies de l'information et de la communication exploitant des réseaux de communication ayant une capacité illimitée de transmettre l'information, a modifié les données géopolitiques. A la société industrielle succède la société de l'information, encore qu'il convienne de noter que cette société est très inégalitaire puisqu'elle est marquée par une forte inégalité entre ceux qui ont accès aux technologies et ceux qui n'en bénéficient que très peu ou pas du tout. Exemple de la « fracture numérique », l'accès à Internet est très variable selon les pays ou les grands ensembles régionaux : près de 70% en Amérique du nord (Etats-Unis, Canada, Québec) ; entre 52 et 63 pour les principaux pays de l'Europe occidentale ; 11,8 % en Asie ; 10,1 % au Proche-Orient et moins de 4% en Afrique noire. Soit au total environ 17,8% de la population mondiale en 2007[22].

En tout cas, la mondialisation et la société de l'information conduisent à une évolution des enjeux pour la sécurité nationale. A côté de la menace traditionnelle d'un conflit militaire ou de la menace sécuritaire (terrorisme), d'autres dangers se sont renforcés à cause des possibilités offertes par les nouvelles technologies. Bien entendu, il ne s'agit pas de faire l'apologie du temps de la lampe à huile et de prétendre que ces technologies sont intrinsèquement perverses. Le développement des sciences et des techniques a

[22] Source : www.internetworldstats.com

souvent une source de progrès et de civilisation : que l'on songe à l'invention de l'écriture ou celle de la roue par les Mésopotamiens (les Irakiens d'aujourd'hui) ; à l'invention du papier par les Chinois, les innombrables inventions (les chiffres, les mathématiques, la médecine, l'optique, l'astronomie, l'architecture, etc.) de la grande civilisation arabo-musulmane, notamment du VII^e^ au XIII^e^ siècle ! Comme toutes les technologies inventées par l'homme depuis les origines de l'humanité, les technologies de l'information et de la communication ne présentent un aspect inquiétant qu'en raison de l'usage intempestif qui peut en être fait. Les aspects positifs des TIC sont incontestables mais celles-ci peuvent être à l'origine de nouvelles menaces, en particulier pour ce qui concerne la sécurité culturelle et la sécurité économique. Il est incontestable que la sécurité nationale, entendue dans un sens large, comprend la sécurité culturelle. Or les TIC posent le problème de la dépendance culturelle, de la pluralité linguistique, de la modification des comportements sociaux et éthiques (diffusion de la pornographie agressive, de la propagande des sectes et plus largement de tout ce qui peut fragiliser les sociétés et porter atteinte à leur identité). La sécurité économique des nations est également en jeu (1) et cette question, relative au problème global de la sécurité nationale, est du ressort de la responsabilité des Etats (2).

### 1- La sécurité économique des nations

Une nouvelle révolution économique « est en marche et elle est fondée sur l'information et la connaissance »[23]. Formidable instrument de progrès, de développement et de croissance, les technologies de l'information et de la communication peuvent donc présenter des risques graves pour la sécurité économique. Tout d'abord, le secteur de l'économie est fragilisé par sa dépendance à l'égard des TIC. Toute perte, toute altération de données informatiques, tout dysfonctionnement peut provoquer des pertes importantes ou, même, mettre en péril une entreprise, un secteur économique ou un Etat. Surtout, les TIC accroissent les vulnérabilités dans un contexte de compétitivité permanente où la sécurité économique est un enjeu essentiel.

Beaucoup semblent tomber des nues en découvrant que la fin de la guerre froide, la mondialisation des échanges et les progrès des technologies de l'information et de la communication n'ont pas conduit au merveilleux « village planétaire » rêvé par les utopistes mais bien à une confrontation impitoyable entre les nations. La réalité est là : la lutte pour les sources d'énergie opposant les puissances, du Proche-Orient à l'Arctique[24] en passant par l'Afrique et le lac

[23] ROUACH, Daniel. *La veille technologique et l'intelligence économique*. Paris : Puf, 2005.

[24] Le 2 août 2007, un bathyscaphe a planté un drapeau russe en titane inoxydable au fond de l'océan Arctique, à 4 261 mètres de profondeur, à la verticale du pôle Nord. Aussitôt après

Caspien ; la possibilité de voir se développer de nouveaux géants économiques (Inde, Chine) inquiète les puissances traditionnelles ; la concurrence pour les marchés n'a plus de limite ; certains tentent d'imposer leurs propres règles du jeu au sein des grands organismes mondiaux que sont l'OMC, la Banque mondiale ou le FMI. Pour reprendre la formule de George Orwell, « la paix c'est la guerre ». En l'occurrence, c'est la guerre économique avec l'un de ses aspects majeurs, la guerre de l'information. En effet, l'information est au cœur du processus de décision, de stratégie et de performance. Les échanges économiques, comme les échanges culturels, sont peu à peu « transférés au sein d'une infrastructure d'information globale, où les organisations sont constituées de systèmes complexes et temporaires d'interactions entre différentes technologies de l'information »[25].

Les systèmes d'information sont donc au centre de l'Intelligence économique, laquelle concerne l'ensemble des actions relatives :

- à la capacité à comprendre son environnement, à détecter les menaces et à anticiper les changements dans un contexte d'hyperconcurrence ;

- à la recherche, au traitement et à la distribution, en vue de son exploitation, de l'information utile aux acteurs économiques ;

- aux actions d'influence au profit des entreprises ou des États,

- à la protection et la sécurité des entreprises et des administrations sensibles.

Eric Delbecque précise que l'intelligence économique est à la fois une culture du combat économique, un savoir-faire composé de méthodes et d'outils relatifs à la veille, à la sécurité économique et à l'influence, et une politique publique visant à contribuer à l'accroissement de puissance par l'élaboration et la mise en œuvre de stratégies géoéconomiques et de sécurité économique, ainsi que par des actions en faveur de la maîtrise collective de l'information stratégique[26]. L'alliage de ces trois composantes « vise à maîtriser et protéger l'information stratégique au profit des acteurs économiques nationaux ».

---

les Etats-Unis, le Canada et le Danemark ont réagi en envoyant des missions dans cette région une potentiellement riche en hydrocarbures.

[25] BAUMARD Philippe et BENVENUTTI Jean-André. *Compétitivité et systèmes d'information*. Paris : Dunod, 1998.

[26] DELBECQUE, Eric. *L'intelligence économique*. Paris : PUF, 2006.

A vrai dire, l'intelligence économique est un terme nouveau qui traduit un concept aussi ancien que les affrontements entre les intérêts des nations mais qui trouve une nouvelle actualité avec les multiples vulnérabilités dues à l'influence considérable des technologies de l'information et de la communication dans le système économique. Confrontés à une compétition de plus en plus forte, les pays industrialisés cherchent à tirer profit de l'information technique et les principales puissances ont, depuis longtemps, développé des systèmes d'intelligence économique et de veille technologique[27], sans compter les actions de renseignement ou d'espionnage poursuivies par certains. Le Japon été le premier, après la seconde guerre mondiale, à faire de l'information, souvent recueillie par tous les moyens, et de l'assimilation puis de l'amélioration des technologies développées par les concurrents étrangers (*benchmarking*), les leviers de son développement dans le cadre d'un partenariat Etat-entreprises citoyens, sous la houlette du MITI (Ministry of International Trade and Industry, devenu Ministry of Economy, Trade and Industry).D'autres pays comme les Etats-Unis, la Grande-Bretagne qui a une ancienne culture du renseignement, l'Allemagne, la France ou, plus récemment la Chine, la Corée ou l'Inde , ont développé des réseaux d'intelligence économique. Si les systèmes d'intelligence économique mis en place par les Etats peuvent revêtir des aspects différents selon les pays, il reste que l'Etat est toujours au centre des initiatives.

### 2- La responsabilité des Etats

L'intelligence économique a trait à la sécurité économique des nations. Quand bien même de grandes entreprises peuvent avoir leur propre système, elle est donc du ressort de l'Etat. Utilisant les mêmes outils de communication et d'information, l'État et les entreprises sont d'ailleurs confrontés aux mêmes menaces. Face à une menace globale, il faut une réponse globale. L'intelligence économique ne peut être laissée à l'initiative de quelques spécialistes, universitaires ou agents spécialisés et cadres d'entreprise. Elle suppose une forte volonté politique et une stratégie d'ensemble mettant en œuvre les orientations fondamentales et des moyens de puissance publique. Seul l'Etat est capable, par l'intermédiaire d'une structure adaptée, avec l'expertise des services de renseignement dans la guerre économique, d'impulser et de coordonner une telle action en partenariat avec les divers acteurs : entreprises, chambres de commerce, secteurs de la recherche, collectivités territoriales (en particulier les départements et les régions).

La sécurité des systèmes d'information est un devoir pour l'État. Il s'agit d'élaborer une stratégie nationale pour limiter les menaces sur la sécurité économique des pays. Une telle stratégie doit poursuivre plusieurs objectifs.

[27] ROUACH, Daniel. *La veille technologique et l'intelligence économique*, ouvrage précité.

a- Tout d'abord, il faut se livrer à un audit des menaces, des vulnérabilités, des points faibles et informer précisément les entreprises et les administrations des risques que les TIC peuvent faire peser sur la sécurité économiques. Cela nécessité la création d'un service national disposant des moyens et des hommes en nombre suffisant. Là encore, les services de renseignement peuvent apporter une aide précieuse en raison de leurs compétences. Par exemple, la Direction de la sécurité du territoire (DST) française mène, dans le cadre de l'intelligence économique territoriale, des campagnes de sensibilisation à l'intelligence économique et à la protection des systèmes d'information, en particulier auprès des petites et moyennes entreprises. En outre, il convient de souligner le rôle du renseignement qui aide les responsables à orienter leurs politiques, les informer des évolutions et des risques nouveaux. Il est notable que des services comme la CIA, le MI6 britannique, les services russes ou chinois, BND allemand ou la DGSE française consacrent désormais une large part de leurs activités à l'intelligence économique et à la veille technologique[28] ou, pour ce qui concerne les services de sécurité intérieur (FBI, MI5, DST) à la lutte contre l'espionnage technologique qui pèse sur les entreprises et les Etats**.** Le recensement des risques doit s'accompagner de la mise en place d'une politique de défense de la sécurité économique visant à protéger tous les secteurs sensibles par des moyens techniques ou juridiques. De telles mesures, qui relèvent du patriotisme économique, impliquent d'avoir une ferme volonté politique et le courage de la mettre en œuvre.

b- la volonté est le maître mot. Il n'y a pas de fatalité du déclin et ne sortent de l'histoire que les peuples qui baissent les bras. A cet égard, le cas du Québec est particulièrement significatif. Après la seconde guerre mondiale, cette Etat francophone de la confédération du Canada avait tout pour dépérir : équipements vieillis, industries en déclin (textile, chaussure, meuble), main d'œuvre peu scolarisée. A partir des années 1960, le gouvernement du Québec a lancé de grandes réformes concernant l'enseignement, la recherche-développement, la création de sociétés d'Etat dynamiques et tournées vers le financement d'entreprise, la mise au point d'une formule de constitution capital de risque qui fournira les assises du développement des entreprises de haute technologie. Le résultat est là : « Aujourd'hui, le Québec est l'un des chefs de file mondiaux dans les nouvelles technologies »[29].

Il est indispensable de conduire une politique favorisant la recherche universitaire et scientifique dans le secteur des technologies de l'information et

[28] Par exemple, le MI6 britannique consacrerait 60% de son activité au renseignement économique.

[29] El TIBI, Zeina. *Le Québec, l'Amérique en français*. Paris : Idlivre, 2002. Traduit en arabe :

de la communication. Le principal danger pour les nations est de laisser se creuser le fossé technologique, d'accumuler les retards et se trouver de plus en plus en situation de dépendance. Le maintien de la compétitivité des entreprises est intimement lié à la sauvegarde de la compétitivité technologique d'un pays. En conséquence, l'Etat doit encore avoir un rôle d'impulsion. Il est d'ailleurs notable que la plupart des technologies de l'information et de la communication ne sont pas nées de l'initiative privée ou entrepreneuriale, elles doivent souvent tout à l'action innovatrice de l'Etat, le plus souvent des services de la défense. Internet est né, à la fin des années 1960, du projet Arpanet du département de la Défense des Etats-Unis et ce n'est qu'à partir de 1993 qu'Internet s'est démilitarisé et ouvert au commerce; le système *Global Positioning System* (GPS) a été également été mis en place par le département américain de la Défense dans les années 1970, tout comme le système GLONASS a été mis au point par l'administration militaire russe ; le système satellitaire doit également tout aux programmes militaires.

Bernard Carayon préconise pour la France la création d'un Commissariat aux technologies de l'information, de la communication et de la sécurité dont la mission consisterait à stimuler le développement d'une filière industrielle et technologique. Il évoque le modèle du Commissariat à l'énergie atomique (CEA), créé en 1945 par le général de Gaulle, qui est « l'exemple type de la réussite industrielle éclatante, suite à une impulsion politique forte. Aujourd'hui, le CEA est en pointe non seulement sur l'énergie, mais aussi sur les sciences du vivant et les technologies de l'information et de la communication ». Le Commissariat aux technologies de l'information, de la communication et de la sécurité permettrait de « mettre en œuvre les orientations définies par le conseil de sécurité économique et d'assurer la mutualisation des financements publics en provenance des différents ministères et des organismes associés »[30].

c- Dans le domaine financier, il est indispensable de d'accorder les moyens nécessaires nécessaire aux activités de recherche-développement. Outre l'effort budgétaire, il est possible de s'inspirer de l'exemple américain d'In-Q-Tel dont les sources de financement associent des fonds publics et privés pour investir dans les technologies essentielles pour la sécurité économique nationale.

d- Plus largement, la coordination de l'action entre le secteur public et le privé est indispensable. Une meilleure articulation public-privé est nécessaire pour ne pas agir dans l'ordre dispersé. Il faut que les divers acteurs nationaux

[30] CARAYON, Bernard. *Rapport d'information sur la stratégie de sécurité économique*. Paris : rapport n° 1664, Assemblée nationale, 2004.

partagent l'information et aient une action commune pour promouvoir l'innovation et les technologies de pointe. Il est notable que les pays qui ont su développer les nouvelles technologies sont ceux où il a été possible de combiner l'action de l'Etat et celle du privé.

e- La coopération internationale doit également être privilégiée entre les Etats. Soit par la mise en place de politique commune de sécurité et de recherche technologique entre des pays alliés, par exemple au sein de l'Union européenne (par exemple, les Etats européens ont lancé le système de navigation par satellite GALILEO qui concurrencera le GPS américain et le GLONASS russe), de l'Organisation de la Conférence islamique, de la ligue arabe ou du Conseil de coopération du golfe arabe. Soit par une action concertée visant à développer une politique d'influence, notamment auprès des organisations internationales où s'élaborent les règles économiques mondiales, pour faire en sorte qu'une régulation pertinente permette de respecter les règles du commerce international, de la transparence des échanges ou de la gouvernance de la société de l'information.

## Conclusion

Quelques mois avant son élection à la présidence de la République en mai 2007, Nicolas Sarkozy affirmait : « Il faut regarder le monde tel qu'il est. Dans une guerre économique qui ne dit pas son nom, les grands enjeux ne peuvent être ignorés en faisant montre de naïveté à l'égard d'une idéologie libérale qui est exposée par certaines puissances qui ne mettent pas toujours leurs actes en conformité avec leurs belles paroles »[31].

La réalité de la mondialisation est une guerre économique qui ne dit pas son nom mais qui menace la sécurité nationale. Ce sont bien les rapports de force et les volontés de pouvoir des grands acteurs de la vie internationale qui donnent le ton dans un contexte d'hypercompétitivité. L'un des facteurs essentiels de cette compétition est le secteur des technologies de l'information et de la communication parce qu'elles sont au cœur du dispositif économique mondiale. La « nouvelle économie » est, en grande partie, fondée des activités économiques essentiellement basées sur les technologies de l'information et des télécommunications : ordinateurs, logiciels, mobiles, cartes de crédit, gestion des données, services, *etc*. Des pays comme l'Inde et la Chine consacrent près de la moitié de leur croissance à leur politique en faveur des TIC. L'économie mondiale vit à l'heure des TIC. Mais celles-ci qui ont naître de nouveaux

[31] Discours à Charleville-Mézières, le 18 décembre 2006.

espoirs, engendrent également de nouvelles vulnérabilités et des dangers d'attaques extérieures contre la sécurité économique des nations et de leurs entreprises. La réponse à ces menaces pour la sécurité nationale doit être une politique globale, cohérente, déterminée, de la veille économique et technologique, de la sécurité économique, de la production, de l'investissement et surtout de la recherche et de l'innovation en matière des technologies de l'information et de la communication, ce qui suppose également de créer une synergie entre recherche civile et recherche de sécurité et de défense. Il appartient à chaque Etat de prendre la mesure de l'enjeu et mettre en place une politique dynamique et volontaire, et, le cas échéant, de développer des programmes communs avec des pays amis ou des organisations régionales