Menaces, Confiance et Technologies

« *La réalité du champ de bataille est qu'on n'y étudie pas ; simplement on fait ce que l'on peut pour appliquer ce qu'on sait. Dès lors pour y pouvoir un peu, il faut savoir beaucoup et bien.* »

Lieutenant Colonel d'artillerie F. Foch, 1903 extrait de ses conférences à l'école de Guerre.

Dans une période où les mots de cyber-guerre sont présents dans la presse spécialisée et font les titres des journaux et hebdomadaires de manière régulière, cette citation traduit bien la réalité quotidienne des opérateurs de télécommunications confrontés à un environnement de plus en plus complexe.

Cette industrie est au cœur de la problématique de la cyber sécurité puisqu'elle construit les autoroutes de l'information et les services offerts à leurs clients véhiculés sur ces infrastructures. Ce métier les rend éligibles à la catégorie d'opérateurs d'infrastructures vitales, et légitime trois questions :

- Quel est le niveau de la menace actuelle et future pour les États et les entreprises ?
- Quels seraient les mesures à prendre pour instaurer la confiance ?
- Face à un constat parfois d'impuissance, quelle évolution technologique de la cyber sécurité ?

Quelle menace actuelle et future pour les Etats et les entreprises ?

C'est une question qui mérite de s'y attarder car elle conditionne la nature et la forme de la réponse et l'évaluation des risques que font les entreprises et les gouvernements.

Pour les états

Force est de reconnaître qu'au-delà des généralités qui sont publiées sur les possibles menaces et les différents modes d'attaque, il n'y a pas de description précise et actualisée de la panoplie d'armes existantes ou en cours d'élaboration chez des adversaires potentiels, à la fois parce que cette activité ne ressort pas de l'activité classique des complexes militaro-industriels et probablement aussi par le manque de capacités de renseignement dans ce domaine qui défie les organisations et les méthodologies actuelles des services de renseignement.

La cyber menace seule, aujourd'hui, n'est pas de nature à mettre à genoux un État. Elle peut créer des problèmes dans son tissu économique, social, industriel, y compris des problèmes graves dans des secteurs comme le transport, l'énergie, les banques, les systèmes de télécommunications. Aujourd'hui cependant les catastrophes naturelles du type tsunami ou cyclone sont largement plus destructrices pour les économies, et testent de manière plus rude la capacité de résilience des États qu'une attaque informatique fut-elle d'envergure.

Les études internes des opérateurs télécoms montrent malgré tout qu'il est possible de perturber sérieusement les réseaux mobiles et fixes, mais neutraliser tous les réseaux de

tous les opérateurs dans un pays donné au même moment pour une période donnée et significative en termes militaires semble un objectif difficile à atteindre aujourd'hui pour un adversaire potentiel.

Force est de constater qu'hormis l'Estonie, petit pays à faible population et à faible niveau de complexité cybernétique, nous n'avons pas d'exemple à nous mettre sous la main comme objet d'études. D'aucuns nous disent que c'est normal puisque si un cas se développait, il s'agirait de la « bombe nucléaire informatique » et que la retenue ou la mise en réserve pour des actions futures décisives prévaut, que l'effet de dissuasion jouera…que l'on recherche un effet de surprise donc que cela n'est pas utilisé mais que cela existe…

Certes, mais comme pour la dissuasion nucléaire, la dissuasion cybernétique ne peut jouer pleinement que lorsque quelques « tests » sont publics et leurs effets suffisamment persuasifs… Les armes - apparemment américano-israéliennes si l'on en croit la presse spécialisée - de type Flame, Stuxnet et la réponse iranienne sur Aramco étaient trop ciblées pour convaincre et avaient des effets finalement limités, même si la prolifération virale qui va en découler ne fait que commencer.

La nature structurellement résiliente des réseaux de télécommunications, la complexité croissante et la constante évolution des cibles à attaquer sur un pays tant soit peu développé où la notion de territoire n'a pas ou peu de sens, la difficulté de la planification de la manœuvre sur un pays de taille significative, les effets collatéraux à peu près certains et les effets boomerang probables rendent aujourd'hui et à moyen terme, cette hypothèse assez irréaliste.

Enfin n'oublions pas que pour faire fonctionner sa structure, tout État moderne possède de systèmes de communication durcis et redondants.

Mais qu'en sera-t-il de cette menace dans le moyen et long terme ?

A plus long terme et cela commence donc aujourd'hui, il faut absolument que les États conçoivent leur infrastructure critique au niveau local et supra national et envisagent celle-ci, - qu'elle soit de transport, de télécoms, d'énergie, d'eau - comme un ensemble systémique, un système de systèmes, dans lesquels ce type de menaces doit être pris en compte dans l'architecture pour obtenir le niveau de résilience souhaité.

Cela suppose un État architecte et normatif et volontariste car la tendance naturelle va aller forcément vers une minimisation des coûts et vers des impasses.

Il faut donc que l'État ou un niveau supranational décide du niveau de la menace, de ses formes potentielles, de ses points d'application, et qu'une méthodologie de réduction des risques coordonnée soit appliquée en liaison avec le secteur privé pour éviter de multiplier à l'infini les réglementations, et affecter la dépense publique et privée de manière rationnelle avec des incitations fortes.

Ce n'est pas tant les dommages directs qui sont à craindre que les dommages dus à des effets cascades non maîtrisés et non anticipés par le pays attaqué et aussi vraisemblablement par l'attaquant.

Ce qui mérite une attention particulière c'est certainement l'internet des objets et le fait que notre monde va reposer sur une seule technologie de communication - l'Internet Protocol - sous toutes ses formes et un nombre très limité d'OS (systèmes d'exploitations) avec une très grande difficulté pour corriger les vulnérabilités de tous ces équipements une fois dispersés dans notre vie quotidienne. C'est une source d'efficacité, de baisse de coût, d'interopérabilité mais c'est l'assurance aussi d'une probabilité plus élevé de « catastrophe » à grande échelle que ce soit de manière volontaire ou involontaire. L'essence même de la résilience, serait aussi de diversifier les technologies.

Les États sont victimes également de l'espionnage. Rien de nouveau, sauf que le cyber espace permet de multiplier presque à l'infini les espions dont l'efficacité s'accroît de manière spectaculaire et assure une impunité presque parfaite à cause des techniques d'anonymisation mises en œuvre.

Les États sont donc vulnérables et peuvent être fragilisés pendant des périodes plus ou moins longues en fonction de leur niveau de compétence technique mais il n'est pas aujourd'hui démontré qu'une victoire puisse être obtenue uniquement par des moyens de cyber guerre.

Pour les entreprises ?

Pour les entreprises la situation n'est pas la même que pour les États. En effet, elles sont fondamentalement plus exposées et menacées car plus fragiles.

Deux mêmes types de menaces coexistent ; le harcèlement et l'espionnage.

Le harcèlement que je qualifierais de douloureux, c'est celui qu'elles subissent tous les jours, c'est-à-dire du déni de service distribué ou pas, des tentatives plus ou moins réussies de vol de données, des fraudes par manipulations de données techniques. C'est un bruit de fond que beaucoup d'entreprises ont appris à gérer, qui occupe voire sature les équipes informatiques mais qui demeure globalement gérable en termes d'impacts économiques.

Bien sûr, de temps en temps cela fait mal. Quelques entreprises se retrouvent faire la une de la presse, ou subissent une « class-action » et de forts dommages en termes d'image et financiers surtout lorsque les données personnelles et notamment bancaires sont volées.

Les autoroutes de l'information sont devenus des coupe-gorges fréquentés par tous les bandits de la terre et le monde des opérateurs de réseaux est passé d'un club de « gentlemen » ingénieurs à celui de hackers sans foi ni loi en compétition acharnée entre eux.

L'espionnage est une affaire beaucoup plus sérieuse et cela peut être mortel pour l'entreprise. Lorsque nous avons affaire à des activités menés par des États ou des cyber-corsaires payés par des États, l'entreprise est vraiment démunie.

Comme le rappellent régulièrement les autorités dans les pays occidentaux, souvent l'hygiène élémentaire n'existe pas au sein des entreprises et les attaques réussies sont souvent très triviales. Il est important de noter que le fond de commerce technique des attaquants n'a pas vraiment évolué si ce n'est par la combinaison plus grande des charges utiles incluses dans les « malwares ». Mais il est clair que des entreprises à haute valeur technologique qui sont souvent celles ciblées ne sont pas capables de résister à des attaques

sur le long terme. La durée de la manœuvre d'approche pour s'infiltrer dans un système d'information est aujourd'hui de quelques heures à quelques mois mais pas plus. Le scénario est simple et mélange souvent de l'ingénierie sociale et de la technique.

L'objectif de ces attaques n'est pas de détruire mais de capter le plus longtemps possible de l'information stratégique donc d'endormir la méfiance des administrateurs.

Au-delà de la perte financière, l'affaiblissement de la compétitivité est manifeste.

A cet égard on peut se demander pourquoi ces menaces ne sont pas prises davantage en compte dans les entreprises ; peut-être parce que les dirigeants ne sont que très rarement sanctionnés par leurs actionnaires sur ces aspects là, et qu'aujourd'hui on choisira délibérément d'améliorer la marge plutôt que de dépenser de l'argent dans la sécurité.

Une prise en compte de la cyber-sécurité dans la gouvernance des entreprises au niveau des conseils d'administration et des Comités exécutifs avec des mécanismes incitatifs permettrait de rééquilibrer les arbitrages financiers des investissements vers la sécurité, dont le cout est relativement faible et l'effet de levier important. Cela a été fait dans le domaine de l'éthique et de la responsabilité sociale d'entreprise, alors pourquoi ne pas y inclure la capacité de se défendre efficacement et de préserver ainsi la valeur de l'entreprise sur le moyen et long terme !

Pour survivre les entreprises ont donc besoin d'un environnement de confiance dans le cyber espace.

Quels sont les mesures de confiance ?

Au niveau des États

Tout d'abord, il serait utile que les États rassurent les entreprises et le monde économique en général. Ils devraient envisager sérieusement de signer un traité de non militarisation du cyberespace et ainsi arrêtent de vouloir transformer le cyberespace en champ de bataille. L'histoire de la piraterie maritime et ses conséquences néfastes sur l'économie européenne entre le 16ème siècle et le 19ème siècle est suffisamment connue et étudiée pour que l'on puisse en tirer quelques leçons.

Les propositions de traité comme celui formulé par les Russes fin 2011 mériterait l'attention. Malheureusement, l'opposition entre des visions divergentes à la fois sur les priorités de traitement des menaces (cyber-crime d'abord pour les uns, cyber-guerre pour les autres), et sur l'utilisation de l'internet comme arme de propagande et de subversion envers des régimes « non-démocratiques », bloque des avancées significatives.

Le ministre des affaires étrangères britannique M. Hague traduisait cette situation en affirmant récemment : *"These are the need for government to act proportionately in cyberspace and in accordance with international law. The problem, however, lays in reconciling such a concept of freedom of expression with traditional notions of political sovereignty"*

Ce qui est clair, et il faut insister sur ce point, c'est que malgré toutes les mesures que l'on pourrait prendre, les infrastructures critiques, essentiellement supportées par des

entreprises privées ne sauraient résister à des États manipulant le cyberespace.

Après le lancement de Spoutnik en 1957, le Comité pour l'utilisation pacifique de l'espace extra-atmosphérique fut créé en 1959 et le « *Traité de l'espace* » entra en vigueur en octobre 1967 après avoir été signé en janvier de la même année. Il aura donc fallu seulement 8 ans pour se mettre d'accord, même si 30 ans après la guerre de l'espace menée par le Président Bush et les essais chinois d'interception réussie dans l'espace extra-atmosphérique l'ont sérieusement écorné.

On peut espérer seulement que cela prendra moins de temps pour celui du Cyberespace que celui du *Droit de la Mer*, une fois pris conscience qu'il faut négocier. Celle-ci interviendra lorsque certains pays après avoir joué aux apprentis sorciers, se verront attaqués sérieusement sur leur infrastructure.

Les menaces de rétorsion militaires classiques que certains proposent, ne sont pas crédibles lorsque l'origine supposée des attaques provient d'un membre permanent du conseil de sécurité.

Puisque l'espionnage est certainement pour les entreprises et les États la forme la plus dangereuse de l'activité d'un adversaire, il est nécessaire de SAVOIR donc d'être renseigné non seulement sur ce qui se passe dans nos Systèmes d'Information et de Communication (SIC) (c'est du contre–espionnage classique) mais en dehors de nos SIC, dans l'underground, dans le monde des corsaires et des États peu regardants…Quels sont les armes qu'ils peuvent fabriquer, quels sont nos faiblesses, que font-ils, que préparent-ils ?

Aujourd'hui malgré des efforts certains, il est nécessaire de développer cette composante.

Au niveau de l'écosystème industriel

Si une paix relative pouvait être négociée dans cet espace, il ne resterait plus qu'à s'occuper du cyber-crime.

Cela pourrait se faire et se fera par :

- Une action sur les normes qui pour le moins sont très peu sécurisées ou plus exactement mettent la sécurité en option. L'IP V6 est à cet égard intéressant, il porte par construction des mécanismes de sécurité mais beaucoup sont en option et il est à parier que peu d'utilisateurs professionnels vont les activer, brisant ainsi la chaîne de confiance.

- Une action sur la gouvernance des entreprises comme indiquée précédemment

- Une action sur la législation dans certains pays pour éradiquer les réseaux de botnets (notamment en Europe) en les détectant parmi les clients des opérateurs internet et télécoms,

- Une action internationale pour d'autres ; pourquoi la Russie et la Chine qui contrôlent si bien leur internet, n'éradiquent-ils pas leur réseau de botnets ?

- Une action sur la sécurisation de la « supply chain » (hardware et software) qui préoccupe les opérateurs télécoms. Pour les opérateurs de télécoms et d' infrastructures critiques, il s'agit de construire par des mesures plus réglementaires

de la transparence avec les fournisseurs. Avec un problème: au sein des pays partageant les mêmes valeurs et du fait de l'asymétrie qui existe entre certains pays pour les fournisseurs de logiciel et de matériel (Microsoft, Oracle, etc)…sont-ils prêts à fournir les informations de manière proactive pour bâtir la confiance… ? et à qui ?

• La modulation de l'avantage cyber dont bénéficient certains états par la présence d'un tissu industriel dominant au moyen d'une utilisation plus massive de logiciels libres,

• Une ingénierie des systèmes préoccupée autant de résilience que de performance.

Une évolution technologique

La comparaison de deux mondes - celui de l'automobile et des systèmes d'information et de communications - peut être riche d'enseignements.

L'accident dans le domaine automobile comme l'incident dans le domaine informatique est souvent défini comme un événement fortuit. Pourtant les deux ne sont pas inévitables et un grand nombre de moyens existent pour lutter contre ces phénomènes.

Pour le premier, l'Union européenne[1] s'était fixé pour objectif de réduire de moitié le nombre de tués sur les routes entre 2001 et 2010, en fait elle est passée de 54302 morts à 30900 soit une réduction de 43%.

Pourquoi pas le même objectif dans le domaine des SIC ?

Cette réduction dans le domaine de l'automobile n'est pas le fruit du hasard mais le résultat d'un travail structurel des constructeurs automobiles et des fournisseurs d'infrastructure, commencé pratiquement depuis le début de la mise en circulation des véhicules automobiles il y a un siècle et centré sur trois aspects ; la sécurité passive, active et prédictive.

La sécurité passive

Elle[2] a été implémentée au travers du design et des fonctionnalités : il s'agit entre 1910 et 1950 de fonctions liées à la vision ; le rétroviseur, les essuie-glaces, les feux de croisement et de brouillard puis les clignotants en 1939. En 1944, Volvo introduit le premier pare-brise feuilleté qui n'éclate pas en cas d'impact. L'introduction de l'électricité et de l'hydraulique va permettre d'introduire des équipements de sécurité ; la commande hydraulique de frein (1921), l'assistance au freinage (Renault 1923), l'essuie-glace à moteur électrique en 1926, le dégivrage du pare-brise (Volvo 1951), le freinage par double circuit (Volvo en 1966).

La tenue de route grâce à la roue à laquelle Continental apporta les sculptures en 1904, Goodyear le roulage à plat avec chambre en 1934 et Michelin le pneu à carcasse radial qui a fait sa fortune à partir de 1946.

1 *European Commission Directorate General for Mobility and Transport*

2 *L'automobile et la sécurité par Valeo [2008]*

Après la vision du conducteur et l'adhérence du véhicule sur la route à grande vitesse et par temps de pluie, les constructeurs se sont intéressés à la protection des occupants en cas d'accident grâce au concept de sécurité active.

La sécurité active

Les crash tests sont apparus au début des années 50 centrés sur le choc frontal et les tonneaux. Au vu des résultats, les ceintures de sécurité 2 points puis 3 points pour retenir le buste du passager ont vu le jour. Par la suite, l'adoption de l'enrouleur automatique, du dispositif pyrotechnique de tension qui réduit celle-ci en cas de collision puis du système de pré-tension en cas de freinage trop fort ont permis d'améliorer encore la sécurité.

Les cellules d'habitacle se sont rigidifiées mais en parallèle les structures avant et arrière avec des aciers déformables qui absorbent le choc dans le temps et l'espace ont été mises en place. Pour protéger le passager, on a déployé la colonne de direction encastrable chez Mercedes en 1966, l'appui tête en 1968 par Volvo, le pare choc à absorption d'énergie en 1971 par Saab puis la barre de protection latérale des portes en 1972 par Saab.

L'airbag a été rajouté en 1973 par General Motors afin de protéger la tête du conducteur, puis est apparu l'airbag passager, l'airbag latéral, l'airbag de genoux et le double coussin avant sur la Lexus IS en 2006.

Non comptant de protéger le passager, les constructeurs sur incitation de la Commission Européenne ont protégé le piéton des chocs éventuels avec un design de la face avant plus verticale et une plus grande distance entre le capot et le haut du moteur.

Au-delà des réglementations, ce sont surtout les organismes regroupant les constructeurs, les assurances, les consommateurs et les gouvernements qui ont fait bouger les choses en instituant des tests normalisés : EuroNcap en Europe, NCAP aux USA par exemple.

La médiatisation de ces résultats a été un facteur puissant d'évolution des constructeurs dans le domaine de la sécurité.

La sécurité prédictive

L'ABS (Anti Block Bracking System) a été introduit de manière fiable par Mercedes en 1978. Il s'agit d'un système très sophistiqué incluant des capteurs de vitesse des roues et un jeu d'électrovannes évitant le blocage des roues. Le système de contrôle de stabilité (ESC Electronic control stability) connu aussi sous le nom d'ESP a pour but d'aider la voiture à prendre la trajectoire souhaitée par son conducteur en cas de début de perte d'adhérence. L'ESP est apparue en 1995 sur une Mercedes Classe S. En plus des paramètres de l'ABS, l'ESP mesure l'angle de rotation du volant, l'accélération latérale et le moment de lacet. Certaines voitures le complètent par le démarrage en côte ou la limitation du roulis de la remorque.

L'éclairage n'est pas en reste, après l'arrivée de l'ampoule halogène puis du premier projecteur à surfaces complexes sur la Citroën XM en 1989, on est passé à la lampe à décharge sous xénon en 1991 chez BMW avec une luminosité équivalente à celle du plein jour. La technologie d'éclairage à LED est maintenant commercialisée depuis 2002 et en

mai 2008 l'AUDI A8 fut la première à être 100% LED, technologie limitant fortement la consommation électrique et augmentant la durée de vie.

L'aide au pilotage a vu le jour, avec l'apparition des radars de proximité capable de détecter les obstacles ou une distance trop faible entre véhicules et l'aide au parking pour se garer tout seul.

Enfin après accident, des dispositifs sont en mesure d'émettre des appels téléphoniques en cas de déploiement de l'airbag. Jumelé à des systèmes de localisation GPS, ils permettent l'intervention des secours même lorsque le conducteur ou les passagers restent inconscients. L'arrivée en 2013 des premiers véhicules connectés à internet devrait offrir des horizons encore plus larges mais des exigences de sécurité renforcées.

Ce panorama de la sécurité serait incomplet sans parler du réseau routier dont les normes ont évolué depuis le profil de la route, la composition de son revêtement jusqu'à la signalisation Le conducteur a été mis aussi à contribution, il est en effet soumis à un certificat d'aptitude obtenu par une formation, un système répressif organisé autour d'un système de points mis en œuvre par des forces de police ainsi que de systèmes automatisés comme les radars sans oublier un système d'éducation fondé sur des campagnes d'information, intervention dans les écoles, nécessité de refaire une formation après la perte de points de permis….En fonction des époques et de l'efficacité, l'état met l'accent sur l'un ou l'autre des éléments du dispositif.

Toute cette évolution qui s'est déroulée entre 1930 et aujourd'hui est remarquable dans la mesure où le prix des véhicules en euro constant est resté stable. A titre d'exemple en France entre 1960 et 2010, le salaire minimum horaire a été multiplié par 3,5 en euro constant alors que le prix d'un voiture de bas de gamme a été multiplié 1,1.

Or un véhicule de 2010 offre une sécurité et un confort qui n'ont rien à voir avec un véhicule des années 60 !

Les enseignements

Quels enseignements peut-on tirer de cette évolution de la sécurité dans le monde automobile dans le domaine de la sécurité globale et plus particulièrement de la cyber-sécurité ?

On peut noter pour l'automobile :

- Le rôle majeur des clients dans l'évolution au travers de la publication/médiatisation des résultats des tests et des essais comparatifs,
- Une démarche permanente des constructeurs pour offrir une sécurité structurelle (security by design)
- Une sécurité passive qui offre des fonctionnalités permettant au pilote de maîtriser son outil tout en accroissant les performances :
- Améliorant de la vision, de la supervision
- Amélioration du comportement (routier) en cas de dégradation des conditions climatiques

• Une sécurité active pour limiter au maximum les dégâts en cas d'accident.

• Une sécurité prédictive qui prend des décisions à la place du conducteur pour maintenir la trajectoire, éviter les obstacles, se garer,

• Un basculement des concepts marketing après le choc pétrolier de 1973 vers la sécurité aux dépends de la vitesse, des consommations excessives et du toujours plus,

• Une maturité certaine après 100 ans de développement de l'automobile qui a su imposer des normes.

Dans le domaine de la cyber-sécurité, les enjeux ne sont pas perçus aujourd'hui à la même hauteur ; la vie humaine n'est pas au centre des débats et le coût affectif des incidents n'est pas comparable à celui engendré par la perte d'êtres chers. On ne peut donc pousser l'analogie trop loin.

On notera malgré tout qu'il est aujourd'hui admis dans le cas de la violence routière que l'impact sur les personnes induit sur les sociétés un impact de niveau très élevé en termes d'image mais aussi de coûts (voir le nombre de morts élevés dans certains pays dans le monde, y compris en Europe).

De manière similaire, on ne peut pas dire aujourd'hui qu'une protection insuffisante de la vie privée et des données personnelles n'a pas d'impact vital sur la personne concernée ; on peut citer par exemple les suicides d'adolescents européens dont la vie s'est trouvée surexposée sur la Toile et dont la presse s'est faite l'écho. De même, une divulgation de données personnelles peut entraîner des conséquences graves sur la sécurité physique d'un VIP, faire perdre un emploi, donner lieu à des pertes financières non prévues, voire même à une perte d'identité amenant un imbroglio dans le monde réel….

Dans le monde de la cyber-sécurité, on peut affirmer qu'il s'agit :

• D'un domaine jeune d'à peine 20 ans ! en pleine crise de croissance et de structuration,

• D'un paysage industriel très éclaté, peu habitué à travailler en symbiose et avec un objectif global de sécurité des données des utilisateurs, des systèmes hétérogènes, provenant de multiple fournisseurs, avec des fonctionnalités de sécurité locales et peu harmonisées,

• D'une sécurité structurelle faible à part quelques produits grand public bien conçus,

• D'une sécurité passive basée aujourd'hui sur la mise en place de logs et de sondes pour détecter mais peu exploitée,

• D'une absence de « crash-test » normalisé au niveau européen sur des architectures cible (hardware et software) et peu de règlementation technique contraignante,

• D'une sécurité active basée sur des IDS/IPS, souvent compliqués à mettre en œuvre, difficiles à intégrer et chers, et à l'expérience, sous-utilisés,

• D'une sécurité prédictive fondée sur des systèmes de détection de comportement encore balbutiants !

L'automobile au cours de son évolution a montré que l'on pouvait intégrer une sécurité maximale tout en maîtrisant les coûts. Une nouvelle (r)évolution avec l'arrivée des voitures connectées s'ouvre qui va rapprocher le monde mature de l'automobile du monde des télécommunications et des technologies de l'information.

Si l'on veut arriver au même objectif de sécurité pour ce dernier, il semble nécessaire de créer un écosystème autour d'intégrateurs capables de gérer les évolutions de nos systèmes à la fois sur les couches réseaux et sur les couches applicatives. C'est une intégration verticale autour de grands groupes et de PME capables de sécuriser l'expérience client qui permettra d'arriver au but. Pour cela une concertation européenne entre les opérateurs télécoms, les fournisseurs d'accès (ISP), les assureurs, les fournisseurs et les usagers semble plus que jamais nécessaire en agissant sur l'ensemble des leviers.

Les États et les entreprises sont confrontés à une dimension supplémentaire dans la complexité de leur environnement. Celle-ci est porteuse de risques sérieux pour les premiers, mortels pour les seconds. Il est donc nécessaire de pouvoir approfondir la réflexion autour de six questions structurantes :

1. quel objectif politique/militaire/économique puis-je atteindre en utilisant le cyberespace,
2. les principes de la guerre y compris économique s'appliquent-ils dans cette espace ?,
3. la liberté d'action (ou préservation de l'initiative),
4. la concentration des efforts (ou supériorité localisée),
5. l'économie des forces (ou juste suffisance), puis-je espérer la victoire sans bataille ?,
6. la surprise (ou exploitation des vulnérabilités adverses), puis-je subir ou créer une surprise stratégique dans ce domaine ?

Enfin osons un pari en prédisant que le futur de la sécurité de l'information va passer par la sécurité des données personnelles sur laquelle les États ou ensemble d'États sont en train de légiférer, parce que l'intérêt des parties prenantes que sont les personnes (impact sociétal) rejoint celui des états et des entreprises (intérêt politique et économique au niveau macro et micro). Cet effort s'inscrit dans une logique à moyen terme qui ouvre le plus de potentialités en termes de développement et de croissance, mais se heurte à la recherche de gains à court terme et à la transformation nécessaire mais lente des comportements .

Auteur[3] : Jean Luc MOLINER

Date : 21 novembre 2012

3 L'auteur est Directeur de la sécurité du Groupe France Télécom Orange.Ses écrits n'engagent pas la responsabilité de son employeur.