Anthologie sur la cyberguerre

Anthologie de textes publiés sur www.huyghe.fr

Guerre informatique, cyberdélinquance, du cyberterrorisme à l'ère numérique : autant de façon de détourner des technologies numériques pour infliger un dommage ou s'emparer d'une ressource par écrans interposés.
Quelle est leur réalité au moment où les formes de la guerre et du terrorisme changent sous nos yeux ?

Qu'est-ce que la guerre informatique ?

Après le cybercrime ou le cyberterrorisme, la cyberguerre définit-il le cadre des nouveaux conflits et affrontements en réseaux?

Car, si la guerre est, suivant sa définition classique, une violence armée, collective, supposant mort d'homme, dirigée par des entités politiques dans des buts politiques, et suivant un système de normes ou de droit qui les rend "justes" à leurs yeux, comment transposer toutes ces notions dans le cyberespace ?

Où passe la frontière avec le cyberterrorisme ? Même si certains groupes l'utilisent à des fins de propagande, il n'a guère provoqué de cyberattentats (en dépit des bruits alarmistes qui prédisaient une destruction des "infrastructures vitales" par écrans interposés).

Alors, la guerre informatique, ou cyberguerre, alias *cyberwarfare* ? Est une utopie ou une réalité ?

Éclipse provisoire ?

Notons d'abord que l'idée a subi un éclipse provisoire.

Plusieurs courants se conjuguaient depuis les années 90 pour rendre vraisemblable l'apparition d'une guerre informatique :

- Les milieux stratégiques travaillaient sur le thème de la Révolution dans les Affaires Militaires : l'idée d'utiliser des armes intelligentes et de remplacer en grande partie la violence physique par des attaques informationnelles y tenait une large place. Les puissances à la technologie la plus avancée pensaient atteindre la dominance informationnelle et donc la supériorité en cas de conflit et la sécurité tout court en appliquant à la guerre les principes de la société de l'information.

- La problématique des armes non létales (qui recouvre partiellement la précédente) avait le vent en poupe. Pourquoi tuer si c'est inutile ? Outre des raisons morales ou la crainte de la sensibilité des médias occidentaux au spectacle des victimes adverses (comme au Vietnam), la technologie semblait pousser dans ce sens : les armes qui soit paralysent les systèmes de communication et de transport adverse, soit son système de décision et de commandement y tenaient une large place à côté des armes capables de maîtriser une foule en colère (ou des

soldats) sans répandre un sang inutile). L'informatique tenait donc une large place dans ces projets.

- La conscience de la fragilité de nos systèmes , le sentiment que nous vivons dans une société du risque, la peur d'un effondrement brusque provoqué par le symbole même de la modernité : de nos prothèses électroniques... tout cela jouait dans le même sens

À l'époque on imaginait facilement qu'un pays voyou engagerait quelques génies de l'informatique pour mener des attaques sur Internet destinées à paralyser une nation entière (les USA pour ne pas les nommer).

Pendant que, dès les années 90, les grands stratèges de la Rand, Arquilla et Ronfeldt, imaginaient des guerres futuristes menées à coups de clics de souris, les administrations successives, que ce soit sous les Bush ou sous Clinton se dotaient de moyens sophistiqués pour parer à toutes les cyberattaques. Ou pour en infliger à l'adversaire. Les scénarios prévoyaient des sabotages contre les moyens de transmission de l'armée, la perturbation de ses réseaux de communication et de commandement.

On y ajoutait aussi des opérations relevant davantage de la propagande ou de la désinformation, mais menées via Internet et destinées à décourager les combattants et l'opinion, susciter des défections... Enfin l'aspect d'attaque contre des infrastructures civiles dites vitales, comme l'approvisionnement en eau ou en électricité, la régulation de la circulation terrestre ou aérienne, complétait le tout.

Au total, cyberguerre était une notion excitante mais floue, une catégorie fourre-tout où l'on rangeait des actions de sabotage et de perturbation sur des réseaux , des centres de décision ou des mémoires avec une action psychologique. Celle-ci était parfois sophistiquée dans sa forme (avec des images numériques truquées) mais très simple dans son principe : faire peur, décrédibiliser le commandement ennemi, encourager la révolte, diaboliser et perturber. La notion s'inscrivait parfaitement dans la logique de développement de la guerre de l'information ou de la Révolution dans les Affaires Militaires .

Puis il se produisit un phénomène de type "Pierre et le loup" : à force de fantasmer sur des périls qui ne se concrétisaient jamais ou d'imaginer des attaques sophistiquées pour vaincre des armées afghane ou irakienne, pas vraiment très férues d'électronique et d'ordinateurs.... Faut-il ranger la cyberguerre dans le carton des vieilleries avec la guerre des étoiles ou les machines à détraquer le climat chez l'ennemi ?

Certes, chacun est de plus en plus soucieux de sécurité informatique : une étude de SOPHOS menée sur un échantillon d'un million de pages, conclut que 28,8 % d'entre elles hébergent des logiciels malicieux (*malwares*) que 19,4 % des pages sont créées par des *spammeur*s, que 4,3 % sont classées comme sites illégaux, notamment sites de *phishing* ou de vente de logiciels piratés. Mais si chacun d'entre nous a perdu quelques minutes, quelques euros ou quelques documents précieux à cause de "pirates" ne fait pas de nous des victimes de guerre.

La guerre informatique qui semblait ne plus concerner que les amateurs de jeux vidéo et cybercrime sous toutes ses formes est pourtant revenue sur la scène..

Après le 11 Septembre, le concept est remis en cause Les vrais kamikazes munis de ceintures d'explosifs et de cutters ou les vrais moujhadjidines qui se cachent dans les montagnes ou sur des toits d'immeubles ont créé une tout autre urgence. Même si l'on annonçait de temps en temps que l'on avait arrêté le "Webmaster d'al Qaïda", et même si l'on fantasmait sur des *hackers* islamistes, pour le moment les kamikazes aux ceintures d'explosifs semblaient plus nous menacer que les génies de l'informatique. L'archaïque était donc plus redoutable que l'informatique ?

Récemment, outre l'affaire géorgienne (voir plus loin) le concept a connu une (relative) nouvelle jeunesse à l'occasion d'une attaque informatique menée contre l'Estonie. On se souvient que ce pays où Internet est particulièrement développé s'était trouvé opposé à la Russie à propos du déplacement de la statue de soldats de l'Armée Rouge à Talinn.

Dans les jours qui suivirent l'Estonie fut victime d'un "déni de service" d'une ampleur exceptionnelle. Les autorités du pays pointèrent aussitôt du doigt les brigades de cybersaboteurs du Kremlin et firent appel à l'Otan pour enquêter sur l'affaire en Mai dernier. Mais, outre que la responsabilité de l'État russe n'a pas été prouvée dans cette affaire, personne n'est mort dans cette cyberguerre et que la paralysie de quelques pages Web pendant quelques heures - encore faudrait-il en mesure l'ampleur réelle - n'a pas plongé le pays dans le chaos. L'impact de l'affaire fut surtout psychologique.

Cyberattaques

Tout au plus pourrait-il s'agir d'une forme relativement bénigne de *cyberattaque,* d'une ébauche de cyberterrorisme, dont on peut se demander s'il était armé, mais le terme de guerre, en dépit de l'inflation qu'il subit en ce moment, semble assez exagéré. Un autre petit indice : l'armée de l'air américaine vient d'augmenter son budget consacré à la cyberguerre et développe de nouveaux centres pour s'y préparer.

La politique des cyberconflits pour reprendre le titre d'un ouvrage récent, reste pour le moment virtuelle et secondaire. En vertu du principe que ce ne sont pas nécessairement les formes du conflit les plus modernes, celles qui exploitent le plus les potentialités de la technologie et qui représentent l'économie maximum de force ou de pertes humaines, qui attirent le plus les acteurs politiques.

Bien entendu, cela n'implique pas qu'il n'existe pas des moyens d'attaque sur Internet ou qu'ils soient inefficaces, bien au contraire.

La notion de cyberattaque ou attaque informatique nous semble pertinente : elle pourrait être commune

- à une utilisation politique-étatique voire guerrière de l'informatique pour mettre un pays à genoux, en économisant les missiles ou en les rendant plus efficaces
-à des attaques terroristes ou para-terroristes en temps de paix (éventuellement commanditées par des États en sous-main) et visant à faire l'équivalent d'un attentat dans le monde virtuel : un dommage accompagné d'un message symbolique pour la victime
- et enfin à des actes de prédation (s'emparer de richesses) ou de destruction ressortant à la délinquance intéressée.

Car cette notion d'attaque reflète une logique technologique.

Qu'il s'agisse d'endommager des mémoires et des systèmes (nouvelle forme du sabotage), de s'emparer de données électroniques (pour les altérer, les copier pour leur valeur commerciale, les utiliser pour tromper…), de se substituer à un propriétaire légitime pour effectuer une commande…, il faut chaque fois penser vulnérabilité et brèche.

Le paradoxe est que les deux caractères qui ont permis la révolution Internet – le numérique et les réseaux, le premier instaurant un code universel, le second permettant la circulation de tous les contenus – sont précisément ceux qui ont fait proliférer les risques. C'est grâce à eux qu'il est possible de s'emparer de biens (numériques comme des bases de données de valeur) ou de produire des dommages par électrons interposés.

Globalement les délits commis sur Internet font deux sortes de victimes (et souvent touchent les deux dans leur mode d'exécution). Les premières sont des cerveaux humains. La loi considère qu'il y a délit dans la mesure où, profitant de l'anonymat du Web, agissant à distance, là où, peut-être, le juge ne peut pas l'atteindre, quelqu'un a, par exemple, publié des contenus diffamatoires, des idées racistes, des propositions sexuelles pour pédophiles ou simplement envoyé des messages abusifs. Le « cerveau humain » peut également subir une tromperie : par écran interposé, on fait croire à X qu'il est contact avec telle administration ou telle autorité pour lui faire avouer son mot de passe, révéler des données confidentielles, ou encore, on lui fait miroiter monts et merveilles pour l'amener à effecteur certaines opérations qui le mettront en situation de faiblesse.

Mais les victimes sont aussi souvent des cerveaux électroniques. Le délit consiste alors casser certains codes, utiliser certains algorithmes, à faire circuler certains programmes dits « malveillants », pour amener une machine faire ce que son propriétaire légitime ne voudrait pas et qu'il ignore le plus souvent : bloquer un système, fonctionner à rebours, donner accès à des données protégées, envoyer certains messages, rentrer dans un réseau d'ordinateurs zombies obéissant à un maître unique…

Notons que dans les deux cas, la force du délinquant réside dans le choix du vecteur qui lui permet d'agir sans être identifié, de passer des systèmes de protection, de diriger des flux numériques (qui peuvent être des flux d'argent) à sa guise.

D'où ce paradoxe : tous les développements d'Internet, y compris celles qui relèvent du Web 2.0 offrent de nouvelles failles. Ainsi, les experts s'attendent à une croissance des attaques via les réseaux sociaux type Face Book, à des détournements des mondes virtuels comme Second life, à des utilisations frauduleuses des téléphones portables. Tout ce qui circule : fichiers MP3, voix passant par Internet (comme par Skype), applications hébergées est l'occasion de prises de contrôle à distance ou de circulation de contenus malveillants ou illicites… Une carte de vœux électronique, un lecteur multimédia, n'importe quelle innovation branchée et conviviale devient ainsi le média par où pénètre l'algorithme pernicieux ou par où s'échappent les données.

C’est assez logique : plus une forteresse a de portes, plus elle est vulnérable. Plus un vecteur est nouveau, moins il est protégé. Plus il y a de standards, plus l’ingéniosité des attaquants trouve à se déployer.

L’État est confronté à cette question des vecteurs

> - à la fois parce qu’il pourrait être lui-même victime - une attaque visant à paralyser les sites ou les systèmes informatiques publics comme cela s’est vue en Estonie, par exemple ou encore un usage proprement militaire d’attaques informatiques pour saboter les systèmes de détection et de protection civils ou militaires..-
>
> - et parce qu’il est de sa mission d’assurer la sécurité des citoyens, et à plus forte raison des institutions ou entreprises stratégiques dont nous bénéficions tous.

Faute de contrôler (et c’est très heureux du point de vue des libertés) les contenus électroniques qui circulent dans le cybermonde. En revanche, comme il est censé réguler la circulation et l’utilisation des armes en fonction de leur degré de dangerosité, il s’efforce d’agir sur les technologies disponibles par vérification, certification parfois interdiction. L’État doit donc affirmer sa souveraineté en interdisant au citoyen d’utiliser certains moyens techniques d’agir en secret (le limitation des moyens de cryptologie pour les particuliers par exemple) et de nuire à distance. Et la puissance publique est proportionnelle au degré de sophistication technique dont disposent les individus. Une nouvelle équation à faire entrer en compte dans le contrat social.

Un défi pour la pensée stratégique

Le problème que pose la guerre informatique est celui d'une violence hybride :

- De petites entités plus ou moins motivées par une idéologie, éventuellement financées par des États, des mafias, ou des acteurs économiques, sont théoriquement en mesure de provoquer un dommage sans mesure avec leur force réelle ou leur représentativité.
- Ce dommage, en termes financier ou psychologiques - sans même évoquer l'éventualité de pertes humaines ou de graves désordres provoqués par des attaques contre des "infrastructures vitales" - sont difficiles à mesurer à l'avance : une petite panne qui sera réparée en quelques heures, une vraie panique accompagnée d'un effet de propagation du chaos ? et dans ce cas ce chaos ne risque-t-il pas de toucher le pays initiateur ou les intérêts des auteurs de l'acte ?
- Et par ailleurs, à partir de quel moment le dommage est-il assez grave pour qu'il faille parler d'acte de guerre ?
- Ce dommage sera, dans tous les cas, très difficile à attribuer à ses véritables auteurs, et pour des raisons techniques et pour des raisons de fond : des phénomènes de sous-traitance, de manipulation ou "croisement" entre crime organisé, intérêts économiques, activisme idéologique et services d'État ne seront pas rares.
- La notion de territoire - attaquant ou attaqué - perd évidemment beaucoup de sa pertinence.
- La variété des attaques constitue un autre défi : prélèvement illicite de données ou paralysie des systèmes attaqués, possibilités de toucher des objectifs militaires, administratifs, économiques par une effet de chaos, simple capacité de "faire perdre du temps" si précieux en

cas de conflit, effet "boule de billard" d'une attaque dans un secteur (les transports, la banque, par exemple) entraînant des conséquences dans un autre...
- La question de l'interprétation des intentions de l'adversaire (vraie guerre accompagnant un vrai conflit, avertissement ou menace, simple "test"..) ne facilite pas non plus le jeu politique. Quelle est sa culture stratégique, quelle logique ?

L'étude de la guerre informatique sera donc une œuvre à long terme, où il faudra être très prudent sur la valeur de l'information qui circule (les victimes peuvent être tentées de minimiser les dégâts, les acteurs de se vanter d'exploits imaginaires et les "marchands de sécurité" de noircir les périls pour justifier leur existence).

Les textes qui suivent ne prétendent évidemment pas résoudre ces problèmes.

Il sont simplement le reflet d'une réflexion au jour le jour sur une donnée stratégique nouvelle en perpétuelle reconfiguration.

Se défendre dans le cyberespace

Que signifie « se défendre » dans le cyberespace ? Pour la plupart, nous savons bien ce qu'est une «attaque». Pour l'excellente raison que nous en avons tous subi une à notre modeste échelle : un virus, un logiciel dit « malveillant », la tentative de saturation d'un site...

Ceci vaut à plus forte raison pour des entreprises (les pertes recensées se comptent facilement en millions à l'échelon d'un pays). C'est, du reste, une expérience perturbante pour les gestionnaires formés à diriger nos entreprises que de se voir être « attaqués » et non plus seulement concurrencés. D'autant plus qu'il peuvent être menacés (outre les formes modernisées de l'espionnage industriel et du vol de propriété intellectuelle) par des offensives que nous pourrions classer en « orientées données ou systèmes » ou orientées sens et contenu. Dans le premier cas l'acteur économique perd d'une façon ou d'une autre du savoir et des capacités (l'intranet ne fonctionne plus, la base de données est altérée..., bref les machines et algorithmes ne remplissent plus leur rôle). Dans le second cas, la menace porte sur des croyances et des opinions (l'entreprise est accusée de fabriquer des produits dangereux, de menacer un équilibre écologique, de se compromettre avec des acteurs politiques suspects, sa réputation est menacée...) et, même si le média joue un rôle crucial dans cette affaire (un « buzz » négatif sur les réseaux sociaux n'est pas exactement la même chose qu'une campagne de presse des années 60), de telles attaques ne peuvent pas être qualifiées de « cyber ».

Les cyberattaques (à distinguer de la cyberguerre, concept discutable) peuvent aussi frapper un État. Le cas le plus connu est celui de l'Estonie en 2007, mais il n'est pas le seul. Et, dans tous les cas, les services gouvernementaux se préoccupent de plusieurs hypothèses, dont la plus mythique, une offensive généralisée à travers Internet, atteignant les infrastructures vitales (vitales parce qu'informationnelles dans des pays fortement dépendant de leurs réseaux de régulation et de transmission numériques). Ce serait le cas extrême - le « Pearl Harbour informatique » ou le « Cybergeddon » (cybernétique + Armageddon). Mais on peut envisager des offensives plus limitées (destinées à exercer une pression sur les autorités), l'accompagnement d'offensives militaires par des attaques informatiques (version moderne du classique recours au sabotage des communications adverses par des commandos infiltrés en territoire ennemi), et, bien sûr, toutes les variétés d'espionnage... Le problème étant aussi qu'il est difficile de distinguer une attaque « économique » (destinée à affaiblir une concurrent) d'une attaque « politique » (destinée à contraindre la volonté d'un État), tant la première répond aux objectifs de la seconde.

L'attaque est manifeste lorsque quelqu'un tente de produire un dommage par ordinateur interposé et via Internet. Le dommage en question peut consister en vol d'information (A pénètre dans la mémoire de l'ordinateur de B contre son gré pour y prélever des données confidentielles), en dégradation de l'information (A ayant pénétré dans l'ordinateur de B rend son contenu inutilisable, ou fait croire à B des renseignements faux, ou encore il amène le site ou l'ordinateur de B à afficher ou transmettre à autrui contre son gré des informations truquées). Ou enfin A peut dégrader le système d'information de B (le réseau de B ne fonctionne plus normalement, ses ordinateurs ne peuvent plus communiquer...).

Toutes ces méthodes peuvent se combiner (A peut prélever des données dans l'ordinateur

de B pour pouvoir ultérieurement en changer le contenu, il peut prendre le contrôle des ordinateurs X, Y et Z pour attaquer B...) ou encore elles peuvent combiner attaques purement informatiques (envoyer un « vers » à sa victime), plus manipulation psychologique (faire avouer un mot de passe par tromperie à un naïf) plus, éventuellement des attaques physiques (couper un câble qui dessert un réseau d'ordinateurs).

En principe, il n'existe que trois façons de se défendre contre une attaque : offrir une résistance supérieure (méthode du bouclier ou de la forteresse), infliger un dommage supérieur (riposte en force), ou exercer une dissuasion supérieure (pour décourager l'idée même de l'attaque). L'idéal étant, bien entendu, de combiner les trois : bon bouclier, bonne épée, et bonne menace.

Forteresses numériques

Il existe d'excellentes études et nomenclatures de toutes ces attaques, de même qu'il existe de remarquables systèmes d'alertes, de prévention..., des organismes, des publications, des sociétés qui se spécialisent dans la cybersécurité, le repérage et analyse des nouvelles offensives. Bien entendu, il serait suicidaire de ne pas se doter des meilleurs experts, des meilleurs antivirus, des meilleures « barrières de feu » (firewall), ni de la meilleure formation. Et si possible, posséder le meilleur système de veille, pour se tenir au courant des périls à venir dans un domaine où, par définition, tout change très vite et où l'on peut s'attendre à subir demain une attaque inédite (« zero day attack » dans le jargon des spécialistes anglo-saxons).
Mais en tout état de cause, la défense « pure », celle qui consiste à opposer une résistance supérieure à la force agressive est ici par nature limitée. Même si elle constitue une étape absolument indispensable pour développer une vraie stratégie globale. Celle de la muraille destinée à subir un siège évoque une vision médiévale : des hommes en arme, cherchant à s'emparer de la forteresse, utilisant des panoplies bien connues, bien visibles et dont l'arrivée peut être repérée à l'avance, s'épuisent vainement et longuement, jusqu'à ce qu'ils se découragent ou que parviennent des secours.

Or, dans l'univers numérique :
- l'attaque est par définition surprenante (et certainement pas annoncée par des déclarations de guerre et des manœuvres d'approche)
- elle ne peut s'exercer que là où l'attaquant à repéré une vulnérabilité : un système de cryptologie insuffisant, une faille humaine, une technologie dépassée, ou simplement une incapacité à gérer plus d'un certain volume de « demandes » (attaque par déni d'accès), un seul défaut sur des millions de lignes de code d'un algorithme, donc là où elle peut agir immédiatement
- c'est une attaque par tromperie au sens large : soit un message envoyé par un être humain, soit une commande activée par un logiciel permet à l'attaquant de pénétrer là où il n'est pas autorisé, de donner des instructions illégitimes, d'apprendre ce qui devrait être caché, d'empêcher de fonctionner une système qui devrait être invulnérable, de remplacer des données par d'autres... et tout cela parce qu'un cerveau, qu'il soit électronique ou humain, a, d'une façon ou d'une autre, reçu des information délibérément truquées.
- toute attaque est nouvelle, ou du moins, il est difficile de se reposer sur l'expérience antérieure : ce qui a fonctionné une fois a exploité une faille que l'on peut a priori penser comblée. Par exemple, pour un nouveau virus on aura recherché un nouveau patch, pour une insuffisance repérée d'un système, on devrait avoir trouvé un système de substitution dans un temps raisonnable, etc..

- Il est en principe difficile de construire des défenses à la mesure de l'attaque, pour l'excellente raison qu'il est difficile d'en prédire la nocivité effective : quelles infrastructures vitales seront vraiment paralysées (et d'ailleurs lesquelles seront visées) ? lesquelles se montreront capables de résilience ? dans quel temps ? la panique se propagera-t-elle ? la paralysie temporaire d'une composante du système global se diffusera-t-elle partout (y compris sans doute hors du pays visé) ? Le tout sur fond de paradoxe du fort : plus on est puissant, ou en tout cas « moderne », plus on est dépendant de ses réseaux informatiques, plus on offre de cibles à d'éventuels agresseurs

Contre-attaques numériques

Bien entendu, il est facile de critiquer les lignes Maginot numériques et de répéter que la meilleure défense, c'est l'attaque. C'est vrai sur le plan des principes et, pour ne prendre qu'un exemple, le livre blanc de la Défense a parfaitement raison de préconiser que notre pays se dote de capacités informatiques offensives.
De même, on peut très bien imaginer la panoplie de rétorsion dont saurait se doter un pays technologiquement avancé ne mobilisant ses forces de sécurité, ses ingénieurs, ses centres de recherche : il pourrait sans doute faire « bien pire » que l'attaquant, surtout si ledit attaquant est un simple groupe de pirates. Sans compter qu'un État peut envisager des moyens non informatiques de rétorsion contre des attaques informatiques.
La vraie question est ici : qui frapper et quelle punition infliger ? En termes politiques, car la question ne peut se poser ici que pour un État, la question est : qui traiter en ennemi ?
En temps de guerre, ou lorsqu'il est fait usage de force ouverte, missiles contre missiles, tanks contre tanks, et que l'attaque informatique est simplement destinée à accompagner une offensive « classique » par une action de sabotage ou d'espionnage, la question n'a guère de sens : paralyser ou infiltrer les systèmes d'information ennemi, le tromper, augmenter « la friction et le brouillard » qui gênent son action, c'est simplement augmenter l'action des forces de destruction par un usage (incapacitant pour l'autre, « capacitant » pour soi) de l'information.
Mais en temps de paix ? À supposer que l'on soit doté de moyens au moins égaux à ceux de l'adversaire (vers, chevaux de Troie, ordinateurs « zombies ») où viser ?
S'en prendre aux infrastructures vitales du pays soupçonné ? Lesquelles au fait, militaires, politiques ou civiles (à supposer que cette distinction ait encore un sens) ? Au risque de frapper dans ce pays des populations ou des organisations qui sont parfaitement innocentes de l'attaque que l'on subit ou que l'on prévient ?
Voire, tout étant connecté sur la Toile, de produire du dommage dans d'autres pays ?
Faut-il le faire ouvertement au risque de provoquer l'indignation de l'opinion ou des sanctions internationales ?
En ce cas, comment prouver que c'est bien un État qui vous a agressé (ou s'apprête à vous agresser) par électrons interposés ? et que cela constitue bien un acte de guerre au sens juridique ?
On sait en effet qu'une attaque peut provenir d'un service d'État (il y en a même qui se dotent tout à fait officiellement de cyberbrigades de combat informatique comme la Chine et les USA), mais aussi d'un groupe de hackers motivés politiquement (éventuellement contrôlés ou encouragés en secret par l'État agresseur en question), voire d'une organisation criminelle (dont les services pourraient parfaitement avoir été loués par un acteur étatique). C'est ce que nous avions nommé le dilemme des 3 M : militaire, militant ou mercenaire ? Même si l'on peut se faire une idée de la chose (dans tel pays, une attaque de cette ampleur n'a pas pu se

développer sans que les services de renseignement ne soient au courant et ne laissent faire quand ils ne financent pas..), cela ne constitue pas une preuve.
Et quand bien même, on saurait qui frapper, une puissance comme la France risque de se trouver confrontée à un paradoxe de riposte graduée (qui n'a rien à voir avec les raisonnements sur la sanctuarisation du pays par la dissuasion nucléaire) : ou bien l'attaquant risque d'être trop fort, ou bien il pourrait être trop faible.
Trop fort : imaginons par exemple que nous soyons persuadés qu'une attaque informatique vienne de Chine, pense-t-on sérieusement riposter par une vigoureuse réplique de virus tricolores et que l'affaire s'arrête là ?
Trop faible ? Mais supposons maintenant que ce soit un « État voyou » du Sud qui ait commandité quelques hackers pour mener une offensive contre nous ? Veut on vraiment se venger en plongeant, disons la Somalie, dans le cyberchaos ?

Tous les problèmes qui précèdent sont probablement solubles, mais ils supposent de se doter préalablement d'une doctrine d'emploi, d'une sorte de gradation des peines et châtiments et surtout d'un excellent système de renseignement pour savoir à qui s'en prendre et où. Rien n'oblige d'ailleurs que ce soit par une riposte (ou attaque préventive) symétrique, informatique contre informatique.

Menaces numériques

Dissuader c'est convaincre un éventuel agresseur (présumé rationnel, oublions le schéma « dissuasion du fort au fou) qu'il aurait plus à perdre qu'à gagner à vous agresser et que vous avez les moyens et la volonté de lui infliger un dommage supérieur en cas de besoin. Or c'est un concept politique.
Il suppose des acteurs ayant des objectifs de puissance identifiés et qu'un certain degré de contrainte, effective ou potentielle, est susceptible de décourager, notamment parce qu'il présente des intérêts visibles et vulnérables.
Mais cela suppose aussi de comprendre clairement ce qu'il vise.
S'agit-il en l'occurrence de gagner un avantage (économique par exemple) indu, de préparer une « vraie » guerre, de tester des défenses ou de faire de la diplomatie musclée en infligeant une punition symbolique ou en adressant un avertissement (ce qui pourrait parfaitement être le cas de l'affaire estonienne) ?
Nous touchons là aux limites de la notion de cyberguerre. Elle a jusqu'à présent été pensée en termes de sécurité (comment s'en préserver) ou de nocivité (quel dommage on pourrait théoriquement infliger à distance, probablement anonymement, et avec des moyens réduits). Or le but de la guerre reste, selon la formule de Clausewitz, et quels que soient les changements techniques, « de contraindre l'adversaire à accepter notre volonté ». La cyberattaque reste donc un moyen de contrainte parmi d'autres, comme la guerre économique ou un soutien discret à un groupe terroriste ou à un mouvement de libération, mais en aucune façon une fin en soi.

ANNEXE I : La nature du cyberespace

Le mot formé de la réunion de cybernétique et d'espace (cyberspace = cybernetics + space en anglais) apparaît en 1984 dans un livre de science-fiction, le Neuromancien de William Gibson. Il désigne « Une représentation graphique de données extraites des mémoires de tous les ordinateurs du système humain » Depuis, l'expression est entrée dans l'usage et sert à désigner le « monde » virtuel qui naît de la connexion des ordinateurs du monde entier échangeant des données. Il nous apparaît en effet comme un espace dans la mesure où nous avons l'impression de nous déplacer « dans » l'information, - par exemple en cliquant sur un lien hypertexte qui nous enverra du site A au site B suivant une proximité sémantique. Il en va de même en participant à un jeu électronique où nous déplaçons un personnage qui va dans plusieurs directions et y rencontre choses et événements nouveaux. Bref, tout se passe comme si nous nous projetions hors de nous-mêmes dans le nouvel espace-temps de la réalité virtuelle. Le cyberespace est en réalité à la fois celui des signaux électroniques circulant physiquement entre des ordinateurs et l'espace mathématique qui se traduit en images sur notre écran. Le tout représenterait à la fois la masse étonnante et toujours en croissance des connaissances humaines mais aussi une structure particulière où tout est directement ou indirectement relié à tout, puisque les informations se renvoient les unes aux autres.
La notion de cyberespace se confond largement avec Internet réseau de réseaux informatiques reposant sur le même protocole de communication (TCP/IP) avec le World Wide Web (dit aussi le Web ou la Toile) qui, lui-même n'est qu'une partie d'Internet. Certains emploient la notion d'infosphère. Ce serait la « sphère virtuelle des contenus numérisés issue de l'interconnexion de l'informatique, des télécommunications et des médias » selon le commissariat au Plan. D'autres étendent la notion au-delà du numérique pour désigner l'univers créé par l'ensemble des documents produits par les hommes. Cela recouvrirait la totalité des productions de l'esprit de notre espèce formulées de façon à les rendre communicable donc partageables par d'autres. L'idée est sans doute inspiré par celle de « noosphère » inventée par Theilard de Chardin en 1947 pour désigner « l'enveloppe de substance pensante » que notre espèce a rajouté à sa biosphère. Ce serait donc le milieu des représentations produites par nos cerveaux, échangeables et dans lequel nous vivons au moins autant que dans notre milieu naturel.

Petite chronique de la cyberguerre
18 Janvier 2010 **Cyberguerre Chine vs Google**

Une cyberguerre entre la Chine et... Google ? Superpuissance contre méga-entreprise ? Cette surprenante nouvelle qui circulait dans la presse vers le milieu de Janvier 2010 mérite un examen un peu plus attentif.
Nous avons suffisamment critiqué le terme de cyberguerre ici pour nous méfier de son emploi médiatique : une guerre sans morts, sans armées, sans différence réelle entre civils et militaires (que ce soit côté acteurs ou côté cibles), sans paix ni traité, sans territoire précis, sans buts politique clairement discernables et qui soit destiné à s'inscrire dans l'Histoire (comme l'annexion d'un nouveau territoire), etc. peut-elle être vraiment qualifiée de guerre ? Certainement pas au sens de Clausewitz ou du droit de la guerre traditionnel.
La cyberguerre, plus souvent évoquée par les stratèges que vécue par des "combattants", pourrait préparer, relayer, amplifier et certains disent même peut-être remplacer, l'action des forces armées par des attaques électroniques contre des dispositifs militaires, étatiques (politiques ou administratifs) mais aussi privés.
Ainsi, le Livre Blanc de la Défense Nationale mentionne la "guerre informatique" parmi les problèmes de la sécurité nationale, affirmant que notre pays doit se doter de moyens de contre-offensive (et pas seulement d'outils de défense et de sécurité), ce qui suppose une doctrine d'emploi. À défaut de guerre, il existerait donc au moins des cyberattaques, menées par l'intermédiaire du Net, produisant des dommages sur des cibles civiles ou militaires.
Leur dangerosité pourrait résulter
- soit du désordre qu'elles provoquent ou provoqueraient (paralyser tout un pays dépendant de ses réseaux informatiques, au moins créer du chaos dans des infrastructures dites vitalescomme des aéroports, des banques, des systèmes d'approvisionnement électronique...).
Donc essentiellement des attaques contre des systèmes
- soit en s'emparant d'un patrimoine informationnel précieux ou de données stratégiques qui devraient en principe être secrètes et protégées par un État souverain. Ce qui ressemble singulièrement à de l'espionnage.
- soit en recherchant un certain impact psychologique sur les décideurs ou la population, en effectuant des actions de propagande ou de désinformation, en accomplissant des humiliations symboliques, ce qui, cette fois suppose de faire circuler des messages trompeurs, provocateurs ou hostiles contre le gré de cet État et en dépit de systèmes de sécurité. Ainsi la "défiguration" du site de l'ambassade de France en Chine au moment des manifestations pro-tibétaines.

Par ailleurs, nous avons également souvent signalé la difficulté de distinguer un "acte" de cyberguerre du cybercrime en général, forme de délinquance qui existe, elle, sans aucune contestation, voire du "cyberterrorisme", qui consisterait à saboter à distance les systèmes informationnels d'un pays ou d'une institution dans un but politique. Dans ce dernier cas, la difficulté est de savoir si l'attentat, ou son équivalent numérique, émane de groupes privés militants ou de services d'État (et plus vraisemblablement de services secrets manipulant des groupes "privés" de pirates informatiques).

Mais cela n'épuise pas la question.
Quand bien même on parlerait de *lutte à travers le cyberespace*, sans employer le mot tabou de guerre, resterait cette nouveauté incontestable : une entreprise menaçant un État qu'elle accuse plus ou moins d'espionnage de se retirer de son territoire et de le priver de sa

technologie. Pendant que l'État qui serait censé se tenir du côté "victime", à savoir les USA, se contente très classiquement de demander des "explications" par les voie diplomatiques.

Que s'est il passé, en effet ?
Version la plus courante : en dépit des 338 millions d'internautes chinois, Google pourrait se retirer du pays en riposte à la "grave atteinte" à la propriété intellectuelle qu'a subi cette compagnie vers la mi-décembre. Les attaques venues de Chine auraient procédé en deux vagues. La première qualifiée d'ultra-sophistiquée s'en serait prise à des codes sources de logiciels Google. La seconde, travaillant de façon plus rustique par "phishing" (attaque qui consiste à "hameçonner" une victime en se faisant passer pour un site officiel comme un banque pour l'amener à vous donner des informations confidentielles). Les victimes auraient été des militants chinois des droits de l'homme. Des "douzaines de comptes" précisait même le responsable juridique de la firme.
Conclusion logique : un pays totalitaire se livre à des manœuvres à grande échelle et persécute des démocrates et Google dont la devise est "do no evil" (ça ne s'invente pas !) réagit en lieu et place de l'État US, freiné par les usages diplomatiques.

À y regarder de plus près, cependant, les choses sont un peu plus complexes :
- L'attitude de Google, d'abord. La société avait passé un accord avec le gouvernement chinois en 2006 pour censurer son moteur de recherche version chinoise (google.cn) Ainsi, sur son portail, quelqu'un qui tapait "place Tien An Men" ne pouvait trouver que des photos officielles et rien qui rapporte les révoltes de 1989. Inutile de dire que l'affaire a fait plutôt mauvais effet et que Google avait à se faire pardonner. Par ailleurs, les mauvaises langues suggèrent que, si le marché chinois est immense, sa rentabilité financière de quelques centaines de millions de dollars seulement n'est pas si fabuleuse à l'échelle de Google. La compagnie de Larry Page and Sergey Brin s'était déjà accrochée plusieurs fois avec les autorités chinoises dont les demandes augmentait ; elle semble même avoir déjà envisagé de quitter la Chine, marché peu rentable et dangereux en termes d'images de marque. La décision pourrait être la suite d'une stratégie réfléchie et non pas une réaction indignée face aux persécutions d'opposants.
Quoi qu'il en soit, le fait que Google se conduise comme une puissance souveraine et sanctionne un État, menant ainsi sa véritable politique étrangère, traduit bien une réalité de la mondialisation : l'émergence des grands acteurs économiques dans le domaine géopolitique, leur capacité de se présenter comme les véritables acteurs de l'histoire, en lieu et place des appareils étatiques dépassés. Voire de les "punir".

- La finalité des deux vagues d'attaque (la "sophistiquée" et la seconde) n'est pas si claire. D'autant que la première vague n'aurait pas touché que le fameux moteur de recherche, mais une vingtaine de sociétés US (voire 35 selon d'autres sources). Tout cela pour se procurer l'adresse ou la correspondance de pro-tibétains ? Difficile à croire. Attaquer Adobe, Northrop Grumman et Dow Chemical, pour prendre quelques noms cités, ne semble pas une façon très logique de persécuter les amis du dalai-lama ou des droits de l'homme. Il semble beaucoup plus logique de penser qu'il s'agit d'espionnage informatique de haut niveau, à but économique et s'en prenant également à des entreprises européennes.
Quant à la seconde vague d'attaques, si elle a touché, selon Google, "des dizaines de comptes mails" d'opposants sur gmail (les adresses électroniques fournies par Google), y compris en Europe, elle pourrait bien ne guère avoir de rapport avec la première. De là à penser qu'il y a, sinon amalgame, délibéré, du moins exploitation médiatique pour mettre sous l'étiquette "défense des droits de l'homme" des réalités qui relèvent plutôt de l'espionnage industriel...

- La culpabilité chinoise, ou plutôt celle du gouvernement chinois, est-elle si évidente ? Sur le plan formel, nous n'en avons aucune preuve. Certes, toujours selon Google, les comptes, tel celui de l'étudiante à Stanford d'origine tibétaine Tenzin Seldon, ont été piratés "depuis la Chine". Mais "depuis la Chine" (traduisez : que l'on à pu remonter jusqu'à une adresse Url se terminant en "cn") ne veut pas dire par les autorités chinoises. Cela signifie que l'attaque est passée par un ordinateur (peut-être infecté et manipulé depuis l'autre bout du monde) situé sur le territoire chinois.

Il y a deux autres hypothèses.
1°) qu'il s'agisse de "faux drapeaux" : des pirates non chinois pourraient parfaitement prendre à distance les commandes d'ordinateurs de ce pays. Des gens qui sont par définition capables de diriger des milliers d'ordinateurs zombies pourraient être assez intelligents pour penser à laisser de fausses pistes
2°) que les attaques partent bien du territoire chinois, mais qu'elles sont issues de groupes de hackers"patriotes", motivés politiquement, mais pas forcément par l'armée chinoise ou ses services.

Bien entendu, il ne s'agit pas d'être naïfs. Il existe des arguments contre la Chine :
- il est difficile de croire que dans un pays aussi surveillé, des "privés" puissent se livrer à ce type d'activités sans que l'État les connaisse, les contrôle, voire les manipule.
- des chercheurs, notamment des Canadiens de l'Université de Munk, pointent depuis mars dernier vers un réseau du nom de Ghostnet, une vaste structure d'espionnage électronique située sur le territoire chinois et qui aurait compris des ordinateurs de services officiels dans 103 pays
- la Chine, souvent désignée par les États-Unis comme responsable de multiples attaques contres les systèmes informationnels, tandis que les think tanks de Washington soulignent que ce pays se dote de capacité "cyberguerrières" en accord avec sa doctrine militaire.

Bref, nous nous trouvons confrontés aux questions récurrentes liées aux cyberattaques :
- celle de l'identification de l'agresseur, mais aussi de la nature de l'agression : à but intéressé (handicaper un concurrent, lui voler ses secrets), politique (exercer une contrainte sur un acteur souverain) ou idéologique et symbolique (défendre et illustrer une cause, en stigmatiser une autre) ?
- celle du "lieu" de l'attaque. Il y a ici contradiction entre la logique classique (une agression part de quelque part et frappe quelque part...) et celle du cyberespace (les attaques ne passent pas clairement par des zones relevant de la responsabilité d'un acteur souverain comme une troupe d'hommes en armes passerait par un territoire où un État est censé exercer son monopole de la violence légitime).

En d'autres termes, il s'agit d'un question de frontières à la fois au sens distinguo entre des catégories (privé/public, politique/économique, militaire/civil), mais aussi au sens topologique, une ligne projetée sur la carte : si la frontière politique détermine deux zones d'exclusivité (ici j'exerce ma justice, j'utilise ma monnaie, j'exerce mon droit, je possède mes armées, j'accueille et interdis, là est ton territoire...), le savoir, le pouvoir et la violence circulent sur Internet suivant leur propre logique.

24 décembre 2009 - **Cyber tsar et cyber menaces aux USA**
Obama et les attaques informatiques

Barack Obama vient de nommer le 22 décembre 2009 un "cyber czar", Howard Smidt après sept mois de réflexion. Ce poste de coordinateur, comparable à celui qui existe dans la lutte contre la drogue ("Drug Czar") correspond à une fonction stratégique de liaison entre agences civiles et institutions militaires (Pentagone, Nsa, Homeland Security) qui s'occupent de cybersécurité, sans oublier la dimension de sécurité économique. En soi, la nomination de cet ancien conseiller de Bush père et ex responsable de la sécurité de Microsoft n'est pas très étonnante.
Comme nous l'avions annoncé, l'actuel président a une ligne politique sur ce point, ligne qu'il exprimait dans un discours du 29 mai : « *Il est clair, désormais, que cette cyber-menace est l'un des problèmes les plus graves, qu'il s'agisse d'économie ou de sécurité nationale, auxquels notre pays est confronté. Il est clair aussi que notre gouvernement et notre pays ne sont pas aussi bien préparés qu'ils le devraient.* » On peut discuter de la justification de ce nouveau poste dans la machinerie bureaucratique US, mais pas de la volonté américaine de résoudre le problème.
Mais au fait quel problème ? Celui des "cybermenaces" ? Certes, personne ne doute que la piraterie informatique ne coûte des centaines de millions d'euros chaque année à des particuliers et des entreprises. Ni qu'il existe des systèmes sophistiqués de vol de données via Internet. Ni même qu'une attaque via la Toile ne puisse paralyser un système complexe. La question est plutôt la coexistence des trois préjudices que peut subir tout système informationnel (et partant, tout particulier, entreprise, administration ou État dépendant de plus en plus de ces systèmes) : la perte d'informations considérées comme des valeurs, le viol d'informations stratégiques et enfin leur altération qui met en danger le bon fonctionnement d'un système.
Ce qui correspond très grosso modo aux trois catégories fort anciennes du vol, de l'espionnage et du sabotage. Les trois se mêlent souvent dans la pratique : pour dépouiller un compte bancaire, il faut, par exemple, s'emparer d'une information confidentielle, et pour cela, probablement, provoquer une dysfonction dans un système de protection. Certains ajouteraient des attaques qui ressortent au domaine l'expression : propagande dite haineuse ou, en tout cas, interdite, actions symboliques consistant à défigurer ou ridiculiser un site adverse, messagerie clandestine, mais nous doutons pour le moment que des crimes ou délits de cet ordre soient d'une gravité qui touche à la sécurité nationale. À noter que si le vol a sa motivation en soi, l'enrichissement, l'espionnage ou le sabotage n'ont de sens que dans l'optique d'une stratégie offensive à plus long terme. Savoir les secrets du concurrent ou de l'adversaire ne prend sens que par rapport à un dessein, économique ou politique. Et saboter (d'une expression née dans les luttes syndicales et qui signifiait "travailler comme un sabot" pour punir l'exploiteur) peut être suivant le contexte le moyen de préparer ou faciliter une offensive militaire, économique ou politique en atteignant ses capacités (à commencer par ses capacités de communiquer).
En d'autres termes face à une offensive contre la confidentialité de données ou de correspondances, il faut se demander à quoi servent ces renseignements et à quel stade ultérieur vise le coupable. Et devant une action destructrice, génératrice de chaos, d'incertitude, de pertes ou de pannes, la question devient : ce dommage est-il destiné à faciliter une offensive d'un autre type (par exemple une attaque militaire ou terroriste "classique") ? ou a-t-il sa fin en lui-même à titre de dissuasion, de provocation ou de représailles ? ce qui voudrait dire qu'il s'agirait alors d'un message à interpréter du type "faites ceci et nous cesserons de paralyser vos

systèmes d'information".

Un second facteur de complexité renforce, en effet, la tendance moderne à fusionner toutes les atteintes à la sécurité d'une Nation, de sa souveraineté, de son intégrité, mais aussi de ses ressources économiques et techniques et de ses habitants en général, dans la catégorie des menaces et agressions (voir notre popre "livre blanc de la défense" par exemple). Parmi les multiples problèmes que pose une cyberattaque (son anonymat et sa non traçabilité apparente, son mépris des frontières qui empêche de savoir d'où elle vient et contre quel territoire elle est dirigée, etc.), celui de la qualification.

Par exemple : est-ce un acte de guerre ? un attentat terroriste ? un acte privé ou une action d'État ? une action de déstabilisation économique menée au service d'un concurrent ? Selon les cas, cela serait censé relever d'un acte de police, d'une plainte devant une juridiction externe, d'une initiative diplomatique ou d'un usage de la violence armée en dessous ou au-delà de la guerre. C'est du moins ainsi que l'on aurait raisonné dans un monde physique avec des frontières et des actions visibles et clairement identifiées (comme de faire pénétrer un corps d'armée au-delà d'une certaine ligne ou de mener une stratégie boursière). Et où l'on savait depuis toujours si l'on était en présence d'un ennemi en tant que membre d'une communauté politique (l'*hostis* des Romains, celui envers qui on peut faire la guerre) ou à titre individuel (l'*inimicus* privé, celui qui nous hait ou que nous haïssons pour ce qu'il est).

Toutes les questions qui précèdent se résument d'ailleurs en une seule : quel rapport avec la souveraineté ? la question vaut du côté de la victime s'en prend-on à un État et à la protection qu'il est censé assurer sur son territoire et à son autonomie afin de l'affaiblir en tant que tel ? ou s'agit-il tout bonnement d'une affaire d'intérêt pécuniaire, comme de déstabiliser un concurrent sur un marché par des moyens déloyaux. L'interrogation vaut aussi quant à l'auteur de l'acte et quant à son intention (politique, délictueuse..) : un service d'État engagent donc la responsabilité des autorités politiques ou un groupe recherchant un but politique ou intéressé (les premiers pouvant d'ailleurs manipuler les seconds, comme le font les services qui encouragent des groupes terroristes pour exercer une pression sur un autre État). Pour en revenir à l'exemple US quelles que soient les sommes que dépenseront les États-Unis, quelle que soit l'utilité d'une coordination civilo-militaire, quelle que soient les technologies défensives dont se dotera ce pays, cela ne servira à rien faute de savoir contre qui se défendre, qui dissuader ou châtier et sur quel plan. Affaire de bons services de renseignement (humain) mais aussi un débat politique à trancher.

5 novembre 2009 - Cyberguerre : désigner l'ennemi

Quand les USA pointent vers la Russie et la Chine

La cyberguerre (classée par le Livre blanc sur la défense et la sécurité nationale parmi les plus graves dangers pour notre pays) ne se laisse pas oublier. Surtout aux USA.

Ainsi, les Américains ont inauguré en Novembre 20009 Centre national d'intégration de la cyber-sécurité et des communications (NCCIC) pour la protection de ses infrastructures vitales dépendant du Secrétariat d'État à la sécurité intérieure. On se sait que le Pentagone possède son "Cybercom" sous l'autorité du Commandement stratégique américain (Stratcom), avec sa structure offensive au nom imprononçable - la *Joint Functional Component Command for Network Warfare* (JFCCNW) depuis 2005. Et que Barack Obama, très soucieux de ces questions s'apprête à nommer un Monsieur Cybersécurité.

Mais les spécialistes d'outre-Atlantique ne se contentent pas de renforcer la défense et d'alerter sans répit sur les conséquences des vulnérabilités informatiques : ils pointent aussi sinon vers des adversaires, du moins vers des suspects.

En Juillet 2009, à l'occasion d'attaques contre des serveurs gouvernementaux, financiers et de médias, en Corée du Sud et aux USA, certains accusaient la Corée du Nord (pays pourtant peu réputé pour son avance technologique et informatique).

La Russie est également montrée du doigt : ses réseaux de pirates (capables de lancer le virus Conficker et disposant de redoutables réseaux de "botnets", les ordinateurs zombies qui obéissent à celui qui les a secrètement infectés) sont célèbres. Et ils seraient pour le moins tolérés pour les autorités. À supposer même qu'elles ne les utilisent pas comme lors de la brève cyberguerre contre l'Estonie en 2007, ou, en 2008, contre la Géorgie.

Mais devinez d'où vient le plus grand danger, dans cette version numérique de la Guerre Froide ? La Chine, bien sûr. Voir un document disponible sur Internet " La capacité de la République populaire de Chine de mener une guerre cybernétique et des des opérations d'exploitation des réseaux d'ordinateurs" par l'Us-China Economic and Security Review Commission. Pour simplifier ce jargon : par guerre cybernétique, il faut entendre l'utilisation militaire des réseaux numériques pour attaquer l'ennemi, et par Computer network exploitation (CNE), des opérations de renseignement menées par les réseaux d'ordinateurs.

Pour être plus simplificateurs, encore, on pourrait considérer que les cyberguerriers chinois se préparaient à faire deux choses principales : ils espionnent (CNE) et ils sabotent (cyberattaques).

Et le rapport d'énumérer les nombreux indices. La doctrine militaire chinoise fait une large place à la "guerre des réseaux électroniques intégrés" ("Integrated Network Electronic Warfare", INEW, encore du jargon). En quête de "dominance informationnelle", elle confère une large place aux attaques par ordinateurs, à la défense et au renseignement par ces moyens high tech. Par ailleurs, la République Populaire se dote de moyens, notamment en multipliant les structures militaires spécialisées et en formant ses experts à cette forme d'offensive dont le principal avantage est peut-être son économie (vieux principe de la stratégie chinoise : pourquoi tuer un oiseau avec une balle en or ?). Enfin le rapport signale les nombreuses connexions entre les services et des groupes de "*hackers patriotes*" qui pourraient bien être les exécutants ou les paravents parfaits pour des opérations de déstabilisation d'un pays adverse (Taiwan ?) sans rien faire officiellement qui puisse vous mener devant le conseil de sécurité de l'ONU.

Ce dernier point est tout sauf négligeable. Ainsi comment juger qu'une attaque informatique constitue un acte de guerre ? La question ne se posait pas quand une brigade en armes

violait une frontière pour aller faire ravage dans le pays voisin. Mais des électrons ? Qui les a lancés ? Quel dommage étaient-ils censé produire et lequel ont-ils réellement accompli ? D'où viennent-ils et que visent-ils ? À partir de quel degré de nocivité des attaques qui ne tuent personne (du moins pas directement) et qui ne font pas couler le sang, qui frappent indistinctement des ordinateurs militaires, publics ou privé, sont elles comparables à une "vraie" bataille ?

Preuve de cet embarras, en 2007, lors de l'attaque menée contre l'Estonie, l'Otan, censée protéger ce petit pays a finalement renoncé à accuser officiellement la Russie (après tout, la majorité des ordinateurs zombies utilisés en cette occasion étaient sur le territoire des USA). Mieux encore : l'organisation internationale a considéré que le dommage subi par l'État membre ne justifiait pas l'application des clauses de défense collective. Façon de dire qu'il ne s'agissait pas d'un acte de guerre (qui n'est d'ailleurs pas défini de façon universelle). Où passera demain la ligne rouge

Toutes ces accusations sont elles vraies ? La Russie et la Chine ont-elles de ces sulfureux projets ? Et si oui, en ont-elles le monopole ?

Dans tous les cas, il va falloir penser la notion nouvelle de "cyberennemi".

La question ne se posera guerre en cas de "vraie guerre" ou d'attaques cybernétiques renforçant dans le cyberespace une offensive par des forces "classiques" (des bombes, des missiles, des tanks..) ; Dans ce cas l'arme des réseaux informatiques sert à perturber les circuits de communication de l'ennemi, à tromper ses décideurs par de fausses informations, à le perturber, plus, bien entendu tout le renseignement acquis en infiltrant le système d'information adverse : c'est le binôme sabotage plus espionnage, version *high tech*, mais au service de la force destructrice.

Mais la plupart des cyberattaques connues ont eu lieu en temps de paix. Elles agissent de façon discontinue (il y a une vague d'attaques, pas des batailles se succédant pour former au total une "guerre" avec début, fin et retour à l'état de paix). Elles n'existent que par l'arme de la connaissance, plus exactement par la découverte d'une vulnérabilité dans le système visé. Elles ne réussissent que par falsification, en trompant soit un être humain soit une machine (un algorithme, un mot de passe..)

Enfin et surtout, elles bouleversent notre vision traditionnelle du rapport entre territoire, frontière et guerre. L'attaque ne vient plus d'un "pays" (ou de ses bases, ou de ses porte-avions, ou de ses colonies, ou d'un territoire quelconque où il exerce sa souveraineté), elle ne passe plus "par" un territoire (un pays allié ou neutre, une zone aérienne, un "couloir"). Enfin et surtout, elle frappe des cibles en profondeur dans le territoire adverse.

Autant de questions nouvelles pour la pensée stratégique

22 octobre 2009 - **Vers la cyberdissuasion ?**

La cyberguerre est un sujet à peu près inépuisable pour les think tanks américains depuis la seconde moitié des années 90. Généralement, leur production tourne autour de deux thèmes :

- l'ampleur du péril - surnommé Pearl Harbour informatique, apocalypse ou "cybergeddon"- pour la sécurité nationale

- l'ardente nécessité de se doter de plus de budgets, de technologie ou d'organismes pour combattre le danger, donc de renforcer le bouclier face à une épée qui change tous les matins

Il est possible que ces deux thèses, qui se situent uniquement dans une problématique de la vulnérabilité, soient vraies, mais leur répétition depuis quinze ans semble plutôt bloquer la réflexion sur le sujet.

Raison de plus pour signaler un rapport de la Rand, par Martin Libicki, un des pontes de la "Révolution dans les Affaires Militaires" : Cyberdeterrence and cyberwar ("cyberdissuasion et cyberguerre").

L'intérêt de ce texte est de poser la question de la "cyberguerre" (pour notre part, nous préférons parler de "cyberattaques") en termes vraiment stratégique, ou plus exactement, de montrer la difficulté de transposer des notions stratégiques classiques dans le cyberespace. Un espace qui, rappelons le, suppose à la fois des choses comme des disques durs ou des câbles que l'on peut détruire, des structures et des réseaux obéissant à des protocoles et dont on peut empêcher ou dégrader le fonctionnement, et enfin de signes que l'on peut imiter, pervertir, etc.., comme une algorithme, un mot de passe, un contenu de message ou des données falsifiés, etc..).

Rappel : il n'y a jamais eu de cyberguerre, avec début et fin des hostilités, enchaînement de batailles, ripostes et offensives, morts, territoires occupés, distinction entre civils et militaires, armistice et paix, désarmement, etc... Pas plus que d'attentat cyberterroriste ayant fait des morts ou des dégâts considérables.

En revanche, il y a eu des milliers et des milliers de tentative de sabotage ou à de l'espionnage par réseaux informatiques interposés et s'en prenant à toutes sortes de cibles et organisations privées et publiques. Il nous semble d'ailleurs que les catégories classiques d'espionnage (voler des informations protégées pour renforcer sa propre capacité offensive) et de sabotage (empêcher un système de fonctionner, produire effectivement du dommage, du désordre, des erreurs, amener la machine ou le dirigeant adverse à prendre de mauvaises décisions...) devraient être davantage prises en compte. Ainsi, dans le monde réel, des acteurs publics peuvent pratiquer ou faire pratiquer l'espionnage ou le sabotage, pour préparer ou accompagner une offensive militaire classique, mais cela ne constitue par une guerre en soi.

Parmi ces milliers d'attaques effectives via Internet, qui ont un coût financier énorme, certaines ont produit des dommages observables sur le fonctionnement de l'appareil d'État, retardant le fonctionnement de sites en les saturant par une technique de type "déni de service" ou pénétrant dans des ordinateurs en principe sécurisés. Nous pensons notamment à la fameuse attaque contre l'Estonie en 2007 et de récentes tentatives (Juillet 2009) contre les USA et la Corée du Sud. Ce sont ces attaques (censées portées sur des infrastructures vitales d'une

Nation) qui sont généralement considérées comme faits de guerre (ou de gravité comparable à des faits de guerre).

Une des questions principales que pose ce type de conflit (outre celui, sémantique et juridique de sa définition précise) est celui de son anticipation. Certes, on peu s'attendre à ce que le bilan d'une guerre "ordinaire" ne serve pas à préparer et gagner la suivante parce qu'il y aura eu changement technique et évolution stratégique entre les deux. Mais les Américains ne jettent pas leurs chars Abrams sous prétexte qu'ils ont été efficaces dans le dernier conflit et que tout changera sans doute au prochain.

C'est pourtant ce qui se passe peu ou prou en matière de cyberconflits : d'abord, la technologie informatique - c'est un lieu commun - évolue chaque jour, une attaque - par "vers" ou cheval de Troie, par exemple - qui est ou serait très efficace aujourd'hui rencontrerait sans doute des défenses adaptées dans trois semaines, du moins si les victimes en connaissaient la nature. Corollaire, ce qui a réussi une fois en matière de cyberconflit, n'est nullement certain de pouvoir être réédité. Nous sommes là devant un problème classique de futurologie : comment raisonner aujourd'hui en fonction d'une invention qui sera découverte demain, à savoir une nouvelle variété d'attaque et/ou de défense ?

Mais le problème d'anticipation est également psychologique et stratégique : dans un cadre "classique", la nation A peut à peu près raisonner sur la façon dont réagirait la nation B en cas de bombardement de sa capitale ou à l'entrée de trois divisions blindées dans une province limitrophe (en première frappe ou en représailles). Un modèle difficile à transposer à une offensive ou une riposte informatique. Il est beaucoup plus difficile d'imaginer :

- le dommage effectif d'une attaque, car celui-ci dépend de facteurs de synergie et de propagation du chaos dans un système (inversement, on peut imaginer, comme ce fut dans une certaine mesure le cas en Estonie, qu'une attaque relativement redoutable dans un premier temps, rencontre un forte capacité de résilience et de substitution en quelques heures). Accessoirement, où s'arrêterait le dommage d'une attaque qui pourrait déborder sur des pays tiers, voire provoquer en bout de chaîne des dommages pour le pays responsable.

- sa finalité réelle (et comment elle serait interprétée politiquement par la victime) : démonstration de force pour exercer une pression, coup déloyal à un concurrent économique, "test" de nouvelles méthodes militaires, prélude à de "vraies" opérations militaires....

- à qui sera attribuée l'attaque (notamment devant l'opinion internationale) : un gouvernement (et en ce cas comment le prouver, car les ordinateurs d'où vient une attaque et qui sont situés sur le territoire de tel pays, peuvent en réalité être contrôlés depuis tel autre)

- comment réagira un pays cible : escalade, riposte de même nature ou par d'autres moyens de contrainte, soumission, appel à des alliés...

En tout état de cause, dans une attaque informatique, tout est affaire de tromperie, qu'il s'agisse de tromper un cerveau électronique - par exemple pour en prendre le contrôle - ou d'un cerveau humain - par exemple pour le pousser à de fausses conclusions sur l'origine d'une attaque. Ce qui implique a priori que l'aspect purement technique du conflit ne peut être séparé d'un important travail de renseignement (qui peut quoi, qui est responsable de quoi, qui réagira

comment...) qui ne peut être confié à des machines.

Le problème se complique encore si l'on se place du point de vue d'un pays cible "vertueux" qui ne désire agresser personne, mais se doter (comme l'esquisse le livre blanc de la Défense pour notre pays) de capacités de rétorsion (ses propres moyens informatiques offensives). Comment ce pays peut-il faire passer un message à d'éventuels agresseurs : si vous attaquez nos systèmes d'information, nous sommes en mesure et nous avons la volonté de vous infliger pire que ce que vous nous ferez ? Et quel "code" de dialogue et de menace peut-il établir avec des interlocuteurs qui vont d'une grande puissance comme la Chine à un État qui pourrait lui-même être faiblement dépendant des réseaux numériques mais avoir engagé un poignée de hackers d'élite ?

Le tout suppose la rencontre d'une intention clairement exprimée (se défendre, punir les agresseurs), d'une capacité technique durable mais aussi d'un mode d'expression clair pour se faire comprendre d'un adversaire dans un jeu aux règles indécises : autant de nouveaux défis pour la réflexion stratégique sur lesquels nous reviendrons sur ce site.

La guerre informatique en Géorgie ? 201-09-2008

Existe-t-elle enfin, se demandent les stratèges ? La vraie guerre informatique, alias cyberguerre, a-t-elle éclaté en Géorgie cet été ? Ou est-ce une emballement médiatique

- Bien sur, il y a des années que l'on annonce un "Pearl Harbour informatique" et les rapports alarmants sur la question fleurissent depuis les années 90 (sans compter les essais à succès ou romans d'anticipation autour du thème : *le monde occidental paralysé par une attaque de pirates informatiques qui créent le chaos, bloquent les banques, les services d'urgence, les communications*...)

- Bien sur, au cours de tous les conflits de ces dernières années qu'il s'agisse du Kosovo ou du Proche-Orient, la presse se fait toujours l'écho d'une "guerre des *hackers*" qui doublerait la guerre réelle. Et cela sans toujours bien distinguer des actions de propagande d'internautes couvrant d'injures ou noyant des spams des sites d'opinion adverse d'une part et, d'autre, part le lancement de virus ou des dénis de service qui touchaient des infrastructures gouvernementales.

- Bien sur, le thème est redevenu d'actualité récemment avec deux événements médiatisés et que nous avions évoqués sur ce site. D'une part des attaques informatiques contre l'Estonie, d'autre part une campagne d'intrusion supposée d'origine chinoise contre des systèmes informatiques de divers pays dont la France.

> Rappelons que :
> * dans le cas de l'Estonie, pays qui dépend effectivement largement de ses structures informatiques, des attaques, qui semblaient provenir du territoire russe, avaient provoqué des perturbations notables dans les systèmes publics. Mais il n'y avait eu ni mort d'homme, ni de dégât qui n'est pu être réparé en quelques jours, ni pertes économiques énormes, ni traces durables et beaucoup avaient interprété cette perturbation - finalement pas beaucoup plus grave qu'un gros orage - comme un avertissement adressé par les Russes à leurs voisins dans un contexte de tension (rappelez-vous : l'affaire de la statue du soldat soviétique)
> * dans le cas des attaques dite "chinoises", il s'agissait davantage de tentatives d'intrusion (pour ne pas dire d'espionnage) que d'une campagne systématique d'attaque.

- Bien sur l'armée américaine et l'Otan se sont dotées de nouveaux moyens "cyberguerriers", tandis qu'en France, le livre blanc de la Défense Nationale, met au nombre de ses priorités la défense de ses systèmes d'information (à commencer par les systèmes informatiques sensibles). Le président de la République envisage même que notre pays pourrait s'engager dans la "Lutte Informatique Offensive".

Ce qui ferait la spécificité des événements actuels, serait que nous assisterions à la première vraie '"frappe informationnelle" menée par une grande puissance en guise de soutien à des opérations militaires. Par ailleurs, ce serait une montée en puissance des Russes en ce domaine : guère efficace pour réduire au silence les sites tchétchènes au début, les services russes seraient maintenant beaucoup plus performants et l'affaire estonienne aurait été un tour de chauffe. C'est du moins ce que prétendent certains forums.

Or que s'est-il passé en Géorgie ? Outre l'habituelle guéguerre sur les forums ou quelques brillantes tentatives pour dessiner les moustaches d'Hitler qui à Poutine qui à Saakachvilli, il s'agit surtout et encore une fois de quelques "dénis de service" sur des sites officiels géorgiens souvent désignées par leur acronyme anglo saxon DDoS (*distributed denial of service*).

En clair, il s'agit de saturer un site officiel sous un nombre de demandes et connexions qu'il est matériellement incapable de soutenir, exactement comme si quelqu'un tentait de bloquer le central téléphonique du Ministère de l'Intérieur en demandant à quelques milliers de personnes de l'accabler d'appels inutiles. La différence est que, sur Internet, cette action peut se faire en employant des "*botnets*" qui sont en quelque sorte des réseaux d'ordinateurs dont on a pris partiellement le contrôle. Ils sont devenus l'équivalent cybernétique de zombies à qui l'on peut "ordonner" de se connecter, sans que les légitimes propriétaires y soient pour quoi que ce soit. La technique du zombie et donc du "DDoS" autrefois assez sophistiquées sont maintenant à la portée de beaucoup puisqu'il est maintenant possible de "louer" de réseaux de botnets. La plupart des utilisateurs utilisent cette technique pour répandre de spams ou des logiciels malicieux, pas pour paralyser un pays.

Du reste, le dommage semble assez modéré. La Géorgie, qui n'est peut-être pas le pays du monde le plus informatisé, a davantage souffert des tanks et des avions russes que des électrons moscovites. La capacité de s'exprimer des Géorgiens et leur faculté de se faire entendre leur point de vue à Washington ou à Paris ne semble guère en avoir souffert.

La fameuse guerre informatique de Géorgie révèle surtout les problèmes habituels que suscite cette stratégie :

- Un problème de traçabilité d'abord. On peut lire dans la presse tantôt que les attaques étaient directement lancées par des services du FSB, tantôt que Moscou aurait fait appel aux services du Russian Business Network, spécialisé dans le piratage informatique et vaguement mafieux, tantôt qu'il s'agit de l'action de hackers "patriotes". Certes on peut toujours raisonner et dire que, comme dans le cas chinois, de telles choses n'ont pu se faire sans l'accord au moins tacite du FSB et des autorités. Mais ce serait tout autre chose que de le prouver devant un tribunal international ou l'Onu. Par définition, de telles attaques sont anonymes et passent par des relais multiples. On ne retrace pas un logiciel malicieux comme on suit le trajet d'un missile sur un écran radar.
- Un problème de mesure du dommage : que quelques sites géorgiens aient été inaccessibles quelques heures est-il une telle catastrophe ? Comment mesurer l'impact d'une cyberattaque dans un monde où par définition tout est en rapport avec tout ? - Un problème d'intention stratégique : à supposer que ces attaques soient bien dirigées par Moscou, quel est leur rôle militaire ou politique ? S'il s'agit de faciliter l'action des armées "réelles" et non virtuelles, on peut douter que ce soit si indispensable. S'il s'agit d'envoyer un message quel est-il ? Que la Russie s'est résolument engagée dans la guerre informatique et qu'elle pourra menacer demain Washington ou Paris ? Ou, tout au contraire, d'éventuels super pirates informatiques du Kremlin n'auraient ils pas avantage à ne révéler que très partiellement leur vraie force de perturbation ?
- Un problème de définition. Une fois encore, nous constatons que la différence entre cyberguerre, cyberterrorisme (c'est-à-dire action de perturbation menée par des groupes "privés" et idéologisés éventuellement sponsorisés par un gouvernement) et cybercrime reste

confuse dans l'emploi quotidien. Sans compter que l'on confond souvent - la capacité de connaissance que fournit Internet (espionnage, pénétration des secrets d'autrui, adversaire ou concurrent), - la capacité strictement offensive qu'il offre (paralyser des systèmes de détection ou de commandement de l'ennemi, perturber de infrastructures vitales civiles ou militaires, provoquer du chaos...) -la faculté d'expression (et éventuellement de censure et de désinformation) que donnent ses instruments - et l'aspect purement technique de ces attaques (introduction de logiciels malicieux, prise de commandement sur des ordinateurs et des réseaux, capacité d'interrompre ou saboter un système de communication...)

Le spectre de la cyberguerre hante-t-il le monde ? 27-05-2008

Après des tentatives censées venir de Chine, après les attaques de 2007 contre l'Estonie qui avaient paralysé une bonne partie des services de ce pays, très dépendant d'Internet, la cyberguerre revient à l'ordre du jour comme nous l'annoncions.

Premier indice : l'Otan vient d'ouvrir à Talinn un centre d'entraînement et d'assistance pour les pays qui se retrouveraient dans le cas de l'Estonie. C'est le second centre de l'Organisation consacré à cet objectif.

Parallèlement, selon le magazine Wired, le thème de la cybersécurité devient une priorité pour le Darpa, l'agence américaine de défense à l'origine d'Internet, mais aussi de projets comme la Total Information Awareness pour lutter contre le terrorisme. Il s'agit cette fois d'une initiative de sécurité nationale, parfois présentée comme l'équivalent pour la sécurité numérique de que fut le projet Manhattan pour la sécurité atomique. Il s'agit d'une part de sécuriser toutes les données numériques passant par les agences fédérales et d'autre part, de crer un "National Cyber Range", sorte d'environnement virtuel destiné à l'entraînement où l'on simulerait des cyberguerres comme on fait des manœuvres sur le terrain. L'idée d'un adversaire tenant de provoquer un "Pearl Harbour informatique", très à la mode il y a une dizaine d'années et passablement éclipsé par la "Guerre globale contre le terrorisme", semble redevenir d'actualité.

Troisième signal fort :l'initiative Impact (I*nternational Multilateral Partnership Against Cyber-Terrorism)*, une organisation internationale de vingt-six pays dont Royaume-Uni, la Russie, l'Australie, le Canada, le Japon... Il s'agit cette fois de faire coopérer les secteurs privés et publics pour lutter contre le cyberterrorisme.

La multiplication de ces initiatives reflète une véritable préoccupation face à des facteurs convergents :

1) Des affaires d'intrusion sur des réseaux officiels américains venues de serveurs chinois (ce qui a pu difficilement se faire sans au moins le consentement passif des autorités) : mais il serait sans doute plus juste de parler de tentatives d'espionnage.

2) La (relative) paralysie qu'a subi l'Estonie engagée dans un conflit symbolique avec la Russie (l'affaire de la statue du soldat russe retirée par les autorités locales). Là encore, il faut relativiser : personne n'est mort dans cette prétendu guerre. Il s'agissait en fait d'un gigantesque "déni de service" qui a paralysé des services, produisant un gêne très importante et des pertes financières conséquences, mais rien d'autre. Resterait à savoir comment interpréter la chose : comme un coup de semonce des Russes contre des ex alliés indocile ? un test ? une punition symbolique ? une message envoyé aux alliés de l'Estonie très pro occidentale ?

3) la prolifération des affaires de cybercriminalité notamment par des ordinateurs zombies.

Raison de plus pour rappeler quelques notions.
Il existe une cybercriminalité : des organisations spécialisées emploient le Net pour opérer à distance des détournements de fonds, des escroqueries ou divers délits qui existent dans le

"monde réel" mais qu'il est beaucoup moins dangereux de pratiquer dans le monde virtuel (ne serait-ce que parce qu'il n'y a pas à se rendre sur le lieux du crime). Leurs techniques, qui sont souvent celles de hackers qu'ils emploient, permettent de contrôler des ordinateurs à distance, de produire certains dégâts, de voler des données confidentielles et de tromper des victimes.

Il existe une utilisation d'Internet par des groupes terroristes pour communiquer secrètement, faire de la propagande, éventuellement pour se procurer discrètement des fonds ou des moyens.... Là encore ce sont des choses que pratiquaient tous les groupes clandestins avant Internet mais qu'ils peuvent faire plus efficacement sur la Toile. Mais il n'y a jamais eu de cyberattentat (et moins encore qui ait fait des morts), tout au plus des sabotages de sites "adverses" par des groupes clandestins idéologiquement motivés (ce qui ne veut pas forcément dire terroristes).

Mais les électrons ne font de victimes sanglantes qui feront la première page des journaux : et le véritable terrorisme suppose des actes de violence contre des gens ou des biens, avec une intensité suffisante pour "répandre un sentiment de terreur", et pour faire parvenir un message clair à l'opinion (les raisons et objectifs politiques de cette violence, des revendications..). Or le Net ne semble ni suffisamment puissant pour le ravage (même s'il peut produire du désordre ou des coûts considérables), ni suffissament clair pour le message (comment être certain, par exemple, de l'auteur de l'attentat, qui tenir pour responsable ?).

Un État pourrait commanditer des opérations de sabotage qui produiraient une gêne considérable pour un autre acteur souverain. En temps de guerre, il pourrait accompagner des opérations militaires par des cyberattaques qui en accroîtraient considérablement l'effet de désorganisation voire de panique sur le structures de commandement ou de sécurité adverses. En temps de paix, il pourrait paralyser certaines des fonctions sur lesquelles repose la bonne marche d'une société (des services d'urgence, des impôts, des régulateurs d'énergie, des systèmes de contrôle ou de communication divers). Peut-être pas au point de détruire ses infrastructures vitales, mais assez pour provoquer quelques heures ou quelques jours de chaos. Et tout cela pourrait se faire sans laisser de preuves formelles ; lorsqu'un État envoie des tanks de l'autre côté de la frontière, il peut difficilement nier avoir accompli un acte de guerre. Lorsqu'il vole des données ou paralyse un service bancaire, il est bien plus difficile de prouver la chose et de le traîner devant le conseil de sécurité de l'Onu. Même si les initiés et les services de renseignement ne se feront jamais d'illusions en réalité.

Au stade actuel, les cyberattaques (qu'il est donc difficile de qualifier d'actes de guerre ou de terrorisme commandité) ont encore une portée limitée. Elles ressortent plutôt à une diplomatie de contrainte : une façon d'exercer une pression sans se dévoiler totalement. La réaction de l'Otan, des USA et de pays membres d'Impact est-elle disproportionnée ? Pas si l'on applique le principe de précaution et que l'on considère qu'il ne faut pas laisser se développer des menaces sur Internet dont le bon fonctionnement est vital pour nos sociétés. Mais il y a aussi derrière tout cela une volonté d'assurer le contrôle du cyberespace et la dominance informationnelle des Occidentaux.

CYBERGUERRE CHINE/USA ? 2007-09-08

Rififi dans le cyber village : des sources officielles américaines accusent une nouvelle fois des "pirates chinois" d'attaquer les réseaux informatiques de la défense américaine. De quoi relancer l'idée d'une cyberguerre par écrans interposés qui pourrait maintenant toucher la France..

Suivant le *Financial Time*s, l'armée populaire de libération chinoise s'est livrée depuis des années à des centaines de cyberattaques contre les réseaux du Pentagone. En Juin dernier, elle aurait réussi à pénétrer jusque dans le bureau de Robert Gates, le Secrétaire américain à la Défense. Cette affaire fait suite à une autre où les militaires chinois auraient tenté d'introduire des « chevaux de Troie » dans les ordinateurs du gouvernement allemand ce qui aurait fait l'objet d'un incident entre Angela Merkel et le premier ministre chinois Wen Jiabao. Avec un pareil dossier, il y a de quoi faire des gros titres, et surtout il y a de quoi raviver une vieille inquiétude de la Défense américaine exprimée depuis les années 90 : qu'un État voyou formant ses propres spécialistes ou engageant des pirates informatiques n'utilise la toile pour mener des offensives contre les réseaux informatiques dont dépend la sécurité nationale. Personne ne prétend que l'armée chinoise soit composée de naïfs ou d'enfants de chœur.

Il est donc tout à fait vraisemblable que comme toutes les armées du monde, à commencer par celle des États-Unis, elle s'est dotée de moyens d'attaque et de défense via les réseaux informatiques. Qui plus est, la doctrine militaire chinoise, ou du moins ce que nous en savons à travers le livre La guerre hors limite (traduit chez Payot), préconise justement ce type d'opérations.
Dans une logique héritée de la tradition stratégique de Sun zi et Sun bi, l'armée chinoise recherche l'économie de moyens, surtout par rapport à un adversaire technologiquement suréquipé. Cette force de l'adversaire éventuel, il faut la transformer en faiblesse. C'est pourquoi, la guerre chinoise de demain sera aussi une guerre de l'information, une guerre économique, une guerre électronique, etc.…
Pour résumer : les Chinois ont l'intelligence, la capacité, et la motivation pour le faire. Est-ce la preuve qu'ils l'ont fait ? D'une part, comment prouver que les attaques contre le Pentagone aient été menées par la Chine ? Quand bien même on pourrait les retracer jusqu'à des ordinateurs sur le territoire chinois, la démonstration laisserait place au doute.
D'autre part, si l'on examine d'un peu plus près la nature des terribles cyberattaques, on s'aperçoit qu'il s'agit d'une pénétration dans un réseau de courriels non protégés réservés aux conseillers politiques du Ministre de la Défense. Dans le cas de l'Allemagne également, les logiciels malicieux que l'on suppose introduits par l'armée chinoise, devaient servir à prélever de l'information, nullement à détruire des mémoires ou des circuits de commandement.

Au fond, si l'on peut parler de cyberespionnage, il n'y a là rien qui ressemble à une agression militaire. Une fois de plus, le terme de cyberguerre semble être utilisé comme un attrape-tout, sexy et sans consistance (après tout, pour qu'il y est guerre, il faut au minimum qu'il y ait mort d'hommes et continuité d'une violence organisée). En revanche, la révélation de ce danger chinois, tombe à pic quelques mois après les accusations lancées contre la Russie qui aurait mené sa propre cyberguerrre contre l'Estonie (en réalité : un déni de service qui avait paralysé des serveurs estoniens pendant quelques heures). L'armée américaine semble

une vivante illustration de l’adage « Tout est clou pour celui qui a un marteau » : elle continue à projeter sur ses adversaires sa propre logique, celle d’une guerre high tech dans la continuité de la "*Revolution in Military Affairs*" .

La lutte contre les attaques informatiques
(à l'occasion du colloque de l'IHEDN du 11 décembre 2008)

La cyberguerre (alias guerre informatique) est entrée, à l'occasion du Livre Blanc de la Défense, au nombre de nos priorités de sécurité nationale. La lutte devient à la fois globale (une sécurité à la fois militaire, économique, technique...) et multidimensionnelle. Le but est de protéger le cyberespace comme l'espace national terrestre, maritime ou aérien, mais à la différence des autres, le premier n'a guère de frontières où poster des sentinelles et des barrières. Là, les notions de distance, de trajet, de limite ou d'étendue perdent tout sens au profit du lien et de l'interconnexion: on y circule non pas mètre après mètre, mais par relation sémantique, de donnée en donnée.
Des exemples récents, notamment en Estonie, ont accéléré cette évolution, en rappelant la fragilité de sociétés dépendantes de leur système d'information à la fois numérique et en réseaux.

Un nouveau ravage

En réseaux, cela implique que tout point dans le cyberespace peut être atteint sans mouvement physique (tel celui d'un corps d'armée ou d'une simple lettre), mais par des relais sémantiques et de multiples vecteurs, ce qui rend difficile l'identification de l'origine. Pour autant, les supports matériels de l'information sont tout sauf secondaires: satellites, câbles, ordinateurs restent des objets physiques dont la destruction ou le sabotage peut avoir de graves conséquences.

La numérisation implique la fragilité des informations sous leur triple aspect de:

- données (stockées hors de notre vue et susceptibles d'être altérées ou prélevées à l'insu du propriétaire légitime)

- messages dont l'État ne peut plus contrôler la circulation sur son territoire

- instructions, dont les algorithmes commandant le fonctionnement de logiciels et de machines.

L'information comporte une autre dimension:la connaissance (la mise en forme de savoirs dans un cerveau humain) et la représentation de la réalité que se font, par exemple, des décideurs peut largement être faussée.

Dans le cyberespace, une attaque peut porter sur chaque dimension de l'information:

- violer un secret, accéder anonymement et à distance à des données protégées, en prendre connaissance, les remplacer

- imposer un contenu: soit propager des messages illicites soit les faire passer par des canaux qui devraientêtre normalement inaccessibles (ainsi: un site officiel pour y « *tagger*» des slogans vengeurs ou en ridiculiser les possesseurs).

- prendre les commandes, par exemple en transformant l'ordinateur d'un autre en «zombie» qui obéit à vos ordres et non aux siens, mais aussi en empêchant le fonctionnement normal d'une chaîne de commandement ou d'alerte.

Pour ne pas se perdre dans les définitions floues de la guerre de l'information, il importe a minima de distinguer l'information «référentielle», description vraie ou fausse de la réalité utile à la décision stratégique, et l'information objet de croyance, dont il importe qu'elle fasse beaucoup de convaincus (propagande, par exemple). De la même façon, dans les attaques informatiques,certaines visent à un effet technique et d'autres à un effet psychologique. Mais il faut aussi distinguer facteur d'amplification et saut qualitatif. Certaines attaques informatiques ne font qu'amplifier ce qui se faisait auparavant par d'autres moyens. Ainsi espionner par ordinateurs ou téléphones 3G interposés, c'est faire plus efficacement ce qui se faisait avec des micros et des agents. Publier de la propagande sur le Web , c'est multiplier l'efficacité du vieux tract. En revanche, créer une panique systémique (songeons à une altération du DNS, le système d'adressage d'Internet), modifier une base de données ou bloquer un système de messagerie, ou faire effectuer à une machine une tâche contre son légitime propriétaire, c'est passer à une autre dimension. Ce n'est pas faire avec des électrons ce que faisait un saboteur avec une scie ou un marteau.

Les attaques se déploient souvent dans ces trois dimensions (savoir, pénétrer, ordonner), même si certaines sont plus orientées vers l'espionnage (prendre connaissance des plans de l'adversaire, ou de s'emparer de son patrimoine informationnel), vers le sabotage (empêcher le fonctionnement normal d'un système informationnel, de détruire ou changer des archives, de troubler un système de messagerie.), d'autres enfin vers la tromperie ou l'effet psychologique.

La cyberattaque est asymétrique et en situation d'information imparfaite (l'anticipation des risque et remèdes dans un domaine où il n'y a guère d'expérimentation préalable). L'attaque peut profiter de la moindre faiblesse (ainsi si un expert dans le monde découvre une faille de sécurité sur une ligne de code parmi des millions,des milliers de gens peuvent être au courant le lendemain et tenter leur chance), la défense, elle, est confrontée au double problème du maillon le plus faible et de la surprise systématique.

Temps et chaos

Une cyberattaque est souvent à deux temps.

Au moment A le possesseur d'un appareil réalise que quelque chose ne fonctionne pas: il ne retrouve plus ses données, une messagerie ne transmet plus, un moyen de contrôle n'a pas détecté ce qu'il aurait dû, une machine a un comportement erratique.

Mais au moment B, on peut mesurer la conséquence de l'attaque «dans le monde réel»: de l'argent a été prélevé, une attaque militaire a pu se dérouler en toute impunité, un service n'a pas fonctionné, un adversaire ou un rival s'est emparé d'un secret technique et l'a mis à profit.

Le facteur temps est crucial. L'efficience d'une attaque informationnelle tient de ce qu'elle fait perdre du temps: les communications reprendront, mais trop tard, les systèmes d'alerte finiront par être rétablis, mais après coup, la panne sera réparée, mais entre temps la panique se sera répandue. La plus emblématique des attaques, le déni d'accès, consiste à bloquer

un site important par une surabondance de connexions. Le principe stratégique reste simple: surcharger un système, comme on ferait sauter un standard téléphonique en faisant appeler de nombreux complices. La victime est comme paralysée par excès de demande.

Prendre du temps dans notre société, c'est souvent provoquer un désordre contagieux: dès que les liaisons sont rompues, dès que l'instantanéité des flux numériques n'est plus assurée, tout grippe. Songeons à nos propres réactions lorsque nous sommes privés quelques heures de notre disque dur, de nos courriels ou de l'accès à nos comptes, multiplions par le facteur systémique, la dimension de l'organisation et imaginons le résultat. Habitués à travailler en flux tendus, parfois formées à réagir instantanément aux sollicitations, et, en tout cas, soumises à une demande de «zéro délai» de leurs utilisateurs, les institutions réagissent mal à tout ce qui crée du délai et de la friction.

Comme,à ce jour, les cyberattaques ont surtout eu lieu sur le papier ou à petite échelle, il est difficile de dérouler toute la chaîne des conséquences qu'aurait une offensive portant notamment sur ce que les Américains nomment des infrastructures vitales. Ils les protègent depuis les années 90, tel le lieutenant Drogo du «Désert des Tartares» scrutant la venue d'envahisseurs qui ne viennent jamais. Il y a en effet environ quinze ans que l'on prophétise un «Pearl Harbour informatique» crédibilisé par force tests de vulnérabilité mais qu'aucun adversaire ne consent à réaliser, faute peut être de motivation, mais sûrement pas d'information.

Reste pourtant que les attaques informationnelles (surtout dans une panoplie complète en synergie avec d'autres offensives économiques, terroristes ou autres) pourraient déclencher une contagion du chaos.

Jusqu'où mènerait le couple panique et désordre? Dans un livre des années 60, Roberto Vacca, extrapolant à partir de cas avérés - pannes d'électricité, embouteillages monstrueux ou paralysie de systèmes bureaucratiques bloqués par des facteurs aléatoires - décrivait leur conjonction et l'emballement qui s'ensuivit. Par exemple,la coïncidence de catastrophes : durant une paralysie du trafic routier, un quadriréacteur tombe sur une ligne à haute tension, d'où black-out, bientôt paralysie et désordre, abandon des villes, effondrement en chaîne, etc.. Plus complexe l'ordre, plus menaçant le chaos. Sans imaginer comme l'auteur un retour au Moyen Age, les effets conjugués de l'affolement et de la dépendance rendraient bien plus nocive une attaque initiale. Ainsi, une cyberattaque qui s'en prendrait à une tour de contrôle d'aéroport, aux transferts bancaires, aux feux rouges d'une ville, au services d'urgence, voire à un cocktail de tout ce qui précède, bénéficierait d'un effet multiplicateur.

Une première préparation contre de telles attaques pourrait donc ressortir à une sociologie fiction, celle des paniques et du chaos systémique. Comment réagiront nos organisations, quel facteur humain d'interprétation et de réaction au phénomène technique? Il faudrait mener parallèlement dans le monde militaire une étude de la dépendance des systèmes informationnels, de la réaction/interprétation des hommes, des réactions collectives en fonction d'une culture communautaire, de la fragilité ou de la résilience des structures..

Ceci sans négliger des réponses beaucoup plus pragmatiques : à attaque technique, défense technique.
Elle commencerait par un vaste travail de veille, à la fois pour connaître l'état de l'art en

matière de hacking par exemple, et pour déceler les attaques informatiques dès leurs prémices, toujours en raison du facteur temps évoqué plus haut.

D'autres réponses s'imposent: sensibilisation, diffusion des connaissances techniques et des alertes auprès des acteurs privés, vérification et diffusion des systèmes sécurisés, recherche et anticipation, renforcement et partage de l'expertise... Y compris en évaluant les dangers inhérents aux technologies émergentes, domaine où la guerre de l'épée et du bouclier évolue très vite, et où la riposte à une attaque subie une première fois est probablement dépassée quand elle est au point. Il faudrait aussiposer des questions comme: quel mal pourra-t-on faire demain avec les nano-technologies? comment pourrait-on exploiter offensivement le web sémantique? etc.
Tout cela sans que des obstacles bureaucratiques n'abolissent les avancées techniques, c'est-à-dire dans une culture du partage d'information. Il faut éviter que chacun fasse la même chose dans son coin, mais aussi que la séparation privé / public dépourvue de sens pour les attaquants ne devienne un handicap pour les défenseurs.

Tout cela figure déjà dans des projets existants, tout comme le développement d'une capacité offensive de réplique à l'agresseur. Ce n'est-ce pas dans ce domaine où d'autres sont bien plus compétents que nous nous proposons de chercher des pistes.

Stratégies de l'ambiguïté

Quel que soit les progrès technologiques de notre future défense, elle n'aura de sens qu'au service d'une stratégie globale.

Si cyberguerre il y a, il est crucial de savoir y transposer ou y abandonner règles et catégories de la guerre .

Or la première caractéristique d'une attaque informatique est son ambiguïté.

•Ambiguïté de sa source.
•Ambiguïté du dommage qu'elle est censée produire.
•Ambiguïté de ses finalités.
•Ambiguïté de sa nature même.

L'ambiguïté de la source tient à la nature de l'attaque: desélectrons laissent moins de traces que des divisions blindées et personne ne les voit arriver sur le champ de bataille. Tracer et attribuer une attaque n'est pas facile: quelqu'un qui sait s'emparer d'un ordinateur distant soit comme cible soit comme vecteur est généralement capable d'anonymiser son action; certes, il reste des présomptions. Il est permis d'imaginer que si tant de milliers d'ordinateurs de tel pays autoritaire se sont mis en action en même temps, cela n'a pas pu se faire sans l'accord au moins tacite des autorités. Mais de là à porter l'affaire devant le conseil de sécurité de l'ONU...
Or il importe de savoir s'il s'agit d'une attaque étatique, impliquant des services et des outils de souveraineté, obéissant à une logique de puissance (affaiblir ou contraindre un autre État, y compris à travers son économie, par exemple) ou d'actes de particuliers. En principe, ils cherchent la satisfaction d'intérêts, dont le plus évident est l'argent (mais il y a aussi la vengeance, le jeu, la recherche de la performance pure...).

Le problème est qu'entre le domaine de la puissance publique et celui de l'intérêt privé se glissent deux figures parfois indiscernables: le militant et le mercenaire.

Nous appelons militant celui qui obéit à un intérêt, mais à un intérêt idéologique. Il croit réaliser une valeur générale par son action, par exemple punir des ennemis de son pays, arrêter un complot impérialiste ou réaliser la volonté de Dieu. Le hacker militant, ou le pirate qui prend un prétexte idéologique pour se livrer à une activité narcissique (compétition pour le plus grand exploit informatique) peut facilement être manipulé par un service.
Quant au mercenaire, en principe un expert privé, il vend sa compétence et rentabilise sa force de nuisance. Ainsi des organisations «louent» des ordinateurs zombies, des algorithmes redoutables, des informations confidentielles à un commanditaire qui peut être un acteur étatique (retour à la case précédente).

Comment obtenir la traçabilité et de l'imputabilité des attaques? Le principe « *id fecit qui prodest*» (à qui le crime profite) ne peut se transposer à des enquêtes algorithmiques par des Sherlock Holmes digitaux. Il y faut sans doute du renseignement humain pour identifier les vrais manipulateurs et si possible prévoir leur prochain mouvement.
Par ailleurs leur stratégie peut être soit de rechercher l'anonymat, soit d'essayer de faire accuser un tiers pour accentuer la confusion, soit de faire savoir qu'ils en sont les auteurs (histoire de faire comprendre la menace) mais sans laisser de preuve formelle.
Là encore, pas de politique de rétorsion ou de dissuasion qui vaille sans travail de renseignement pour savoir qui décourager ou qui punir. Le renseignement ne doit pas révéler seulement sur qui a fait, mais aussi qui peut et qui veut faire. Entendez qu'il s'agit aussi d'étudier les intérêts politiques, matériels et idéologiques, les stratégies (voire les doctrines d'emploi), les vulnérabilités des éventuels agresseurs.

Seconde grande question: comment évaluer un ravage qui ne se mesure ni en provinces perdues, ni en milliers de morts, ni en nombre de batailles. Quel est le dommage réel (et qui nous informera sur cela objectivement sans avoir intérêt à dissimuler ses vulnérabilités) et où s'arrête-t-il, éventuellement au-delà des intentions de l'auteur. On peut, par exemple imaginer que dans un monde interconnecté les conséquences d'une attaque sur une base de données, un système bancaire ou autre ait des conséquences y compris sur le pays de l'agresseur. Estimer le dommage réel est une première nécessité. Par exemple pour juger s'il s'assimile à un acte de guerre. Peut-il y avoir mort d'homme? A priori on l'imagine mal (mais que serait une guerre qui ne tuerait personne?), même si, au bout de la chaîne des conséquences d'une cyberattaque, quelqu'un peut effectivement mourir, par exemple à cause d'une paralysie des systèmes de secours médicaux.

Peut-il y avoir destruction matérielle (au moins sous son aspect le plus évident: une perte financière considérable)? À partir de quel ravage, une attaque informatique est-elle violence grave contre les choses assimilable à un attentat?

La perturbation organisationnelle que nous évoquions (notamment par l'enchaînement perte de temps, chaos, panique) ne pose pas moins de questions d'évaluation. Qualifiera-t-on de catastrophe nationale ou d'acte de guerre un service public qui ne fonctionne pas un jour, mais qui, le lendemain, peut être bloqué aussi gravement, mais légalement cette fois par une grève.

Enfin la dimension de l'humiliation symbolique (évidente par exemple dans l'affaire

estonienne s'il s'agissait bien de répondre à un autre acte symbolique: le retrait de la statue d'un héros soviétique), ou de la recherche de l'effet psychologique (peur, contrainte, démoralisation) n'est certainement pas la moins délicate à estimer.
Par ailleurs, comment appliquer des notions d'ordre public à de tels dommages qui commencent souvent par frapper des infrastructures privées?

Mais la mesure du dommage (surtout l'estimation à la source avant que le péril ne se développe) ne vaut rien sans réaction immédiate et appropriée. sans méthode pour limiter la contagion du désordre, maîtriser l'arme de l'information, rassurer, reprendre vite le contrôle, garantir la résilience de nos systèmes informationnels. En clair: il faut inventer un mélange de défense civile et de gestion de crise adaptée aux nouvelles menaces à l'échelon privé et public.
La question se complique si nous envisageons une attaque informatique comme un pistolet à un coup: en révélant sa technique d'attaque, l'agresseur renseigne la victime sur les contre-mesures et court le risque de se heurter la fois suivante à des contre-mesures. Peut-être faut-il donc tout réinventer à chaque fois, et surtout ne pas risquer une guerre de retard

Victoire et châtiment

Troisième domaine: l'évaluation des buts recherché par l'attaquant. Qui est l'ennemi et quel est son critère de la victoire? Faute de réponse, il n'y a ni préparation ni riposte appropriée.
Or il faut chaque fois considérer plusieurs hypothèses:

- l'attaque vise-t-elle à un avantage compétitif (s'emparer d'un secret industriel ou autre, déstabiliser un concurrent, faire baisser son action en bourse, retarder un projet de recherche pour la défense...)?

- est-elle la préparation ou l'accompagnement d'une autre offensive (militaire, économique, terroriste...)? Voire l'annonce d'actes plus graves que son effet premier?

- sert-elle à exercer une pression, agir sur l'opinion, à lancer un avertissement? Une cyberattaque peut devenir un instrument de«diplomatie digitale musclée»,un avertissement à un État (hypothèse qu'il ne faut pas écarter dans le cas de l'Estonie, par exemple, mais moins vraisemblable pour la Géorgie où les tanks et les AK47 ont volé la vedette aux électrons).

S'ouvre ici le domaine du décideur politique: juger de la nature de la menace et celle de la riposte.À lui de choisir une doctrine d'emploi pour les moyens de rétorsion voire à lu de la faire connaître (il n'y a guère d'effet dissuasif si l'adversaire ignore le risque). Au politique d'interpréter et de fixer une stratégie globale.

Ce qui nous ramène en conclusion sur ce par quoi on aurait tout aussi bien commencer: la nature hybride, asymétrique et largement aléatoire de la cyberguerre.

Est-ce une guerre? Au sens clausewitzien d'une effusion de sang qui sert à imposer sa volonté à un acteur politique, cela est douteux.

Sans débattre s'il faut au moins un acteur étatique sur deux pour faire un guerre, celle-ci requiert plusieurs conditions:
- un degré de violence létale (une guerre qui ne tuerait personne serait-elle autre chose qu'une

manœuvre ou une menace?)
- des armes, des outils conçus pour détruire un corps humain
- un caractère collectif: la guerre oppose des communautés, pas des individus
- une certaine continuité (sinon il faut parler d'une simple bataille)
- une finalité politique durable (établir ou agrandir un État, signer un traité, imposer un pouvoir sur un territoire...), bref établir un nouveau rapport permanent et réécrire l'histoire
- une conscience historique et éthique des acteurs. Elle se manifeste notamment par leur conviction qu'ils exercent une violence juste (juste à leurs yeux, bien entendu), juridiquement normée, soumise à des règles différentes de celles du temps de paix (droit, voire devoir de tuer des gens envers qui l'on n'a aucun différend personnel, par exemple).

Il est évident que la présence de chacun de ces éléments est pour le moins douteux dans la cyberguerre telle que nous l'avons décrite qui s'en plus souvent à des choses et à des informations qu'à des gens, qui se pratique avec des médias, qui ne dure guère et ne se prête pas à des développements durables et dont nous ignorons enfin si elle possède cette valeur symbolique à l'égard de ceux qui la pratiquent. À ce propos, il serait d'ailleurs intéressant, si cyberguerre il y a, de se demander ce que serait une *cyberpaix*.

La référence au cyberterrorisme n'est pas plus éclairante. Si le terrorisme se situe quelque part entre «guerre du pauvre» (lutte armée d'un groupe qui n'a pas d'armée, justement) et «propagande par le fait» (un acte de violence, l'attentat, pour faire passer un message de menace, radicalisation, punition, avertissement, défi, etc...), une cyberattaque ressemble certes à un attentat, mais où il y manquerait l'élément de proclamation ou revendication propre à l'attentat terroriste. La composante publique voire publicitaire du terrorisme (faire mourir pour faire savoir) semble ici faire défaut.

Le rapprochement avec l'activité criminelle n'aide pas davantage (même si l'attaque informationnelle est forcément en infraction avec le droit du pays victime) dans la mesure où les acteurs peuvent être des États.

La cyberattaque peut en effet combiner l'effet de contrainte politique, de proclamation symbolique et d'acquisition d'un avantage pratique.

Conclusion

La guerre informatique- ou plutôt les offensives informatiques - rentrent dans la catégorie des nouveaux conflits ou des nouvelles violences, opérations de maintien de la paix et dites «autres que la guerre», terrorisme d'État dissimulé, résistance armée ou guérilla, désordres dans des zones de non droit, affrontement armés de groupes privés, guerre dite économique ou hors limite. Il faut prendre acte de cette dispersion ou hybridation du conflit.

Pour riposter il faudra prendre en compte cette pluralité: toutes les dimensions psychologique, culturelles, idéologiques, stratégiques, prospectives et, bien sûr techniques. Acte conscient d'un acteur humain, la cyberattaque, au moins autant que de la technique qui agit sur les choses, ressort à une pragmatique qui agit sur les gens.

CYBERTERRORISME, CYBERCRIME...
CYBERATTAQUES...

Le cybercrime est un des «mythes fondateurs» d'Internet, une de ces représentations imaginaires qui précèdent souvent l'éclosion des possibilités techniques.

Parallèlement à l'utopie du réseau générateur de prospérité, de liberté démocratique et d'expression créative pour tous, les premiers développements du Web ont été accompagnés, voire précédés, d'un discours alarmiste. Depuis les dernières décennies du XX° siècle, parallèlement à l'attente du Big Brother étatique / électronique, est née une autre figure plus confuse. Celle de l'attaquant par écran interposé.

Elle stimule nos craintes et notre obsession de la sécurité. Pour caricaturer : un *hacker* boutonneux lance un virus qui paralyse tous les systèmes de communication et de commandement de la planète (certains parlent du «*Cybershok*» ou de "*Pearl Harbour informatique*"), pendant que les mafieux nous volent nos numéros de carte bleue et que des pédophiles nazis islamistes répandent leur sale propagande.

Le cyberespace apparaît à la fois comme une zone dangereuse où rôdent des entités agressives et mystérieuses et comme une territoire disputé et à conquérir.

Bien entendu, les choses ne se sont pas exactement passées comme cela (encore que certains virus comme «*I love you*» ou «*Red code*» aient authentiquement coûté des milliards de dollars). En fait, le cybercrime – ou plutôt la cyberdélinquance, une imputation qui figure désormais dans nombre de codes pénaux et de traités internationaux – se présente s sous des formes très différentes.

Tantôt il s'est traduit par de petits inconvénients que nous subissons dans la vie quotidienne : spams, tentatives grossières d'escroquerie, paralysie temporaire de nos ordinateurs. Tantôt, l'événement qui fait la première page des journaux : l'annonce d'une « cyberguerre » lancée contre l'Estonie (un pays particulièrement en pointe dans l'usage quotidien des techniques numérique), puis contre la Géorgie ou encore l'affaire de la Société Générale (s'il est vrai qu'un "bidouillage" de codes permettait à un simple employé de créer cinquante milliards d'argent virtuel, d'un gagner quelques millions un jeudi et d'en perdre cinq milliards un lundi).

La notion vague de "cyberattaques" profitant de vulnérabilités technologiques recouvre souvent des activités communes obéissant à des logiques différentes.

Ces activités communes sont :

1) l'emploi des mêmes panoplies et techniques qui seront décrites plus loin. Une brigade "cyberwar" de l'armée attaquant le système de courrier électronique d'une autre armée, un spécialiste des réseaux engagé par une mafia pour réaliser une escroquerie afin de faire payer quelques dollars à des milliers d'internautes, ou un "script kiddie" (un apprenti hacker découvrant les joies du piratage informatique) utilisent les mêmes instruments (des logiciels malveillants, des botnets...) ; ils doivent recourir au même anonymat, franchir les mêmes

"firewalls" (les "barrières de feu" qui protègent les systèmes informatiques), casser des mots de passe

2) le vol d'information. À un moment ou à un autre l'attaquant, soit par un procédé électronique sophistiqué, soit par astuce (par un coup de téléphone en se faisant passer pour un autre), soit en achetant l'information à quelqu'un qui l'a déjà volée, va savoir quelque chose qu'il ne devrait pas être autorisé à connaître : un mot de passe, le contenu d'une base de données... Ou, ce qui revient au même, il va avoir accès à des algorithmes qui devraient être protégés ; il pourra ainsi prendre le contrôle d'un ordinateur à distance.

3) la perturbation. L'attaquant va détruire ou rendre inopérant un système. Il peut effacer une base de donnée, infecter par un virus tout un réseau, effectuer un déni d'accès qui consiste à rendre un site inaccessible. Dans les cas le plus grave, on peut imaginer, comme l'ont fait certains romans d'anticipation, qu'il rende inopérant le système de contrôle aérien d'un aéroport, plus l'alerte de la police et des hôpitaux, plus les transferts bancaires, plus les feux rouges, plus.... Mais dans tous les cas il y a création d'un élément délibéré de chaos, d'un dysfonctionnement.

4) les stratégies du faire-croire. Soit que son but soit de propagande ou de proclamation, soit qu'il at besoin de déisinformer sa victime, de se faire passer pour un autre, de créer une illusion..., il est rare que l'attaquant ne compte pas sur une réaction psychologique, sur un effet d'influence ou de persuasion.

Cela dit le cybercrime semble obéir à des logiques différentes et souvent mêlées :

- Logique militaire ou paramilitaire du ravage. Il s'agit d'infliger un **dommage** à l'adversaire, par attrition et désorganisation : États réalisant ou sponsorisant des actions d'espionnage, de sabotage ou de paralysie d'infrastructures cruciales, parallèlement à une éventuelle action de propagande (qui, elle ressortirait plutôt à la catégotrie plus générale de la guerre de l'information). Cette logique est bien celle de la guerre : causer une perte (de temps, de coordination, de fonctionnalité, d'argent, de réputation...) à l'entité adverse dans une perspective de victoire politique (lui imposer sa volonté). À noter qu'une telle «guerre» peut être menée aussi bien par des acteurs publics (un service secret ?) que par des acteurs politiques « privés » comme un groupe terroriste (sans oublier l'hypothèse où les seconds sont manipulés ou engagés par les premiers). Une de ses composantes est l'acquisition d'une supériorité sur l'adversaire (l'espionner et perturber ses systèmes) dans la perspective de pouvoir mieux le frapper (lui envoyer des missiles qui n'auront pas été repérés par son système d'alerte par exemple), l'autre de créer directement le dommage (paralyser un service public, paniquer la population).

- Logique d'intérêt où il s'agit tout simplement de gagner de l'argent. Ceci peut se faire de manière directe en s'emparant de richesses numériques telles de coûteuses bases de données ou en faisant dépenser des petites sommes à de nombreux internautes. Mais la stratégie peut également être indirecte. Ainsi lorsqu'un acteur économique recourant à l'équivalent électronique de l'espionnage industriel s'assure un avantage sur un concurrent pour conquérir un marché ou encore l'affaiblir à travers sa réputation ou la fonctionnalité de ses systèmes. -

- Logique (certains diront : illogique) des passions privées. Pour répandre leur croyance ou leurs goûts (culturels, voire sexuels), pour le plaisir de réaliser un exploit, une vengeance, de simples particuliers peuvent violer notre intimité, des secrets, produire des dommages, engendrer du désordre, sans en retirer vraiment d'autres profits que narcissiques et sans autre objectif politique qu'un vague prétexte idéologique du genre "dénoncer le système oppressif".

Ces trois logiques dépendent d'une autre, celle de la technique, y compris à l'ère du web 2.0.

En effet la synergie "numérique + réseaux" (un code unique permettant de traiter texte, image, sons, algorithmes et d'autre une interconnexion de tous avec tous) est intrinsèquement porteuse de dangers :

- Elle permet d'agir à distance. Si certains ont célébré Internet comme un monde "sans frontière" ou chanté la dématérialisation de notre univers, il faut rappeler qu'agir à distance ce peut être agir anonymement, sans les risques de la délinquance qui suppose un contact physique, et souvent du pays où la législation est la moins répressive. Il est même possible voire facile d'emprunter une fausse identité derrière la protection du réseau et de l'écran pour "pénétrer" dans des zones interdites : bases de données confidentielles, centres de paiement ou de commandement, etc. Agir à distance signifie aussi que, dans le cybermonde, il existe de multiples voies d'accès : les électrons peuvent passer par d'innombrables voies (et de multiples vecteurs qui ne sont pas seulement les ordinateurs, mais aussi les smartphones, les lecteurs MP3, les ondes de Blue Tooth ou du Wifi, etc.). Leurs cibles peuvent être soit des cerveaux humains (pour leur adresser des messages illégaux, trompeurs pour les escroquer...), soit des cerveaux électroniques (pour y prélever ou y altérer du contenu, pour les paralyser ou y prendre le pouvoir). Agir à distance peut s'accompagner d'agir à retardement (comme dans le cas où l'on fait pénétrer dans un ordinateur un "rootkit" qui y exécutera sa fonction dite malveillante plus tard).

- Une économie de l'immatériel rend de nombreux biens numériques plus désirables : soit pour leur valeur purement informative (comme une invention ou un plan stratégique qu'il y a intérêt à espionner), soit pour leur valeur commerciale (certaines bases de données qui se revendent). Si ces biens sont désirables quelqu'un va tenter de s'en emparer

- L'informatisation implique la multiplication des centres de commandement, régulation, contrôle qui fonctionnent hors de tout contact direct avec un être humain (les logiciels qui donnent des instructions par leurs algorithmes hors de notre vue en sont un très bon exemple, comme les systèmes de monitoring informatisés). D'où une nouvelle stratégie. Or ces centres (voir plus haut) sont accessibles par de multiples vecteurs si bien que nombre d'actes de cyberdélinquance peuvent être décrits comme des prises de pouvoir à distance : A émet sur l'ordinateur ou le téléphone de B (souvent sans qu'il le sache) des instructions qui se traduiront par une perte (d'argent,

de confidentialité), par un dommage (le système sera paralysé) ou par des opérations qui servent les intérêts de A (ainsi l'ordinateur de B est transformé en "zombie" esclave avec de nombreux autres et sert à attaquer collectivement le système C qui est la vraie cible).

- Enfin, dans une société dite de la connaissance, la délinquance informatique est elle aussi "basée sur la connaissance". Celui qui connaît une faille sur un programme ou un système peut y commettre des actes malveillants. Et comme, il peut transmettre cette connaissance à qui il veut, nos systèmes de sécurité informatique dépendent forcément du maillon cognitif le plus faible.

Par ailleurs, il y a un contraste entre la vulnérabilité de nos sociétés (ou la facilité théorique de nuire par écrans interposés) et, d'autre part, l'absence de véritable cyber-attentat. Les frappes électroniques pourraient être trop sophistiquées ou trop peu rentables en tant que spectacles et symboles , pour le moment

Nos sociétés *high tech* sont intrinsèquement fragiles dans la mesure où elles confient à des mémoires électroniques distantes et à des logiciels plus ou moins protégés par des barrières sémantiques (comme la cryptologie) le soin de gérer des fonctions essentielles. La perte ou l'altération de données, l'usage déviant de systèmes d'information ont en eux même un potentiel de chaos. Il serait proportionnel à l'invisibilité de ces actions et à l'interdépendance des divers moyens de régulation et d'échange.
Par ailleurs nul ne songe à nier l'ampleur et l'efficacité de la criminalité informatique,
- soit qu'elle réalise plus facilement sur Internet des délits pratiqués « dans la vraie vie » (emprunter une identité, menacer, voler des secrets..),
-soit qu'elle invente des actions nocives qui ne peuvent exister que dans le monde numérique comme un déni d'accès ou une prise de contrôle à distance.

Or, au moins à l'heure actuelle, on a vu des groupes terroristes faire de la propagande sur Internet, échanger des messages, recourir parfois aux mêmes méthodes que les cybercriminels pour voler ou faire transiter l'argent dont ils ont besoin… Mais, si l'on excepte quelques «tags » ou actions similaires sur des sites officiels (et encore, il s'agit là plutôt d'activisme), il n'y a jamais eu de *cyberattentat*.
Personne n'est jamais mort d'une attaque par électrons ou mail, alors que des bombes explosent et tuent quotidiennement. Nous poserons que le terrorisme demande à la fois un ravage d'une certaine ampleur (de plus en plus souvent, la mort d'homme, car les dégâts matériels ne semblent suffire qu'aux organisations les moins virulentes) et la propagation d'un message d'une certaine clarté (il s'en prend toujours à des cibles symboliques et leur inflige un châtiment qu'il estime juste ou nécessaire, même si nous parlons de victimes innocentes). Dans ces conditions, les organisations terroristes, qu'elles soient religieuses, indépendantistes ou autres, semblent ne pas avoir franchi ce seuil.

Ceci peut s'expliquer par des motifs techniques (la difficulté de provoquer de dommages assez importants pour engendrer de la terreur). Mais il faudra aussi examiner l'hypothèse du « déficit symbolique ». Un moyen de sabotage électronique peut avoir une grande valeur militaire, mais, justement, le terroriste veut plus que des résultats militaires. Il recherche un impact psychologique, il veut donner un sens symbolique clair à son action (il a frappé les

tyrans ou les ennemis de Dieu, il s'en prend à des idées et à des principes en tuant des gens, etc.), il lui importe que le sens de son acte et la publicité de son intention soient parfaitement lisibles. Que l'on prenne le critère du dommage ou l'ordre de la valeur « exemplaire », un attentat numérique semble encore prématuré. Ceci est particulièrement vrai pour des gens qui disposent d'un tel « capital » de kamikazes prêts à se faire sauter tous les jours pour provoquer lumière, chaleur, sang, morts et spectacle. Ce qui ne nous garantit nullement qu'il en sera toujours ainsi.

Obama et la cyberguerre (10 décembre 2008)

L 'intérêt d'Obama pour tout ce qui touche aux technologies de l'information et de la communication est notoire : le président qui ne se sépare jamais de son Blackberry et qui a fait campagne sur Twitter a, du reste, annoncé son intention de nommer un *superministre* du numérique (un « tsar » disent les Américains). Les démocrates pourraient réviser et amplifier la mystérieuse *Comprehensive National Cybersecurity Initiative* de l'administration Bush, dont on sait surtout qu'elle était très secrète.
Un des premiers dossiers que le tsar trouvera sur son bureau risque d'être celui de la cyberguerre ou guerre informatique.
C'est ce que pense un des principaux *think tanks* spécialisé dans les questions stratégiques, le Center for Strategic and International Studies, un des fleurons de K Street. CSIS vient de publier « *Securing Cyberspace for the 44 th Presidency* », étude lancée en août 2007 après une « vague de redoutables attaques dans le cyberespace ».
En effet, cette année-là, le Département de la Défense, celui du Commerce, la Nasa et autres institutions (jusqu'à la Présidence elle-même) avaient souffert d'une série d'intrusions. Or, même s'il s'agissait davantage d'espionnage que de cyberguerre, et même s'il n'a pas été possible de mettre en accusation une puissance étrangère, ces incidents, combinés aux pertes des entreprises américaines en matière de propriété intellectuelle, ont remis en lumière la fragilité intrinsèque d'un système numérique en réseaux dont dépend tout un pays. Ceci dans un contexte où les USA se préoccupent beaucoup des capacités de la Chine et de la Russie en matière de cyberguerre.
En Mars 2008 également, dans le cadre du *Homeland Security,* le NCSD (*National Security Cyber Division*) avait lancé un exercice dit « Cyber Storm II », sorte de *kriespiel* simulant une attaque sur Internet et destiné à évaluer les réactions des autorités et du secteur privé à ce type d'attaque. Les résultats ont nourri l'inquiétude croissante des spécialistes.
Est-ce si nouveau ? Pour la petite histoire, l'auteur de ces lignes se souvient d'avoir visité les bureaux de CSIS l'été 2001, accueilli fort aimablement par un des chercheurs vedettes de l'institut (non, ce n'était ni Madeleine Albright, ni Henri Kissinger, ni Eward Luttwak dont les noms figuraient sur des portes de bureaux voisins).
Mon interlocuteur insistait sur deux thèmes à l'époque :
- le grand danger vient des jihadistes installés en Afghanistan et dans les zones tribales du Pakistan qui vont lancer une vague d'attentats dans le monde - il faut mettre la priorité sur la cybersécurité, l'autre grande vulnérabilité de nos sociétés (on ressort de CSIS les bras chargés de brochures sur la prochaine cyberguerre).
À croire que le monde n'a pas tellement changé en sept ans.

En 2008, donc, CSIS plutôt bipartisan, remet en vedette la lancinante question de la stratégie globale de sécurité du cyberespace. Ce serpent de mer ressort depuis les années 90 :
- faut-il créer une agence centrale chargée de protéger les réseaux nationaux tout en respectant les libertés civiles ?
- la Maison Blanche ne doit elle pas proclamer une politique globale de sanctuarisation des infrastructures numériques critiques ? -
comment traiter simultanément les aspects technologiques et d'ordre public, mais aussi diplomatiques, militaires, économiques, sans oublier le renseignement ?
- Comment concilier l'aspect domestique et international du problème ?

Il y aura d'abord sans doute des changements bureaucratiques : la nouvelle administration pourrait créer un Bureau National du Cyberespace pour la coordination tandis que le Conseil National de la Sécurité se doterait d'un directorat spécialisé. Les partenariats privé/public devraient aussi se développer sous forme consultative, d'échange d'informations ou de recherche commune.
L'accent serait mis notamment sur les normes et les certification en matière de sécurité informatique, parallèlement à la diffusion de guides, normes et conseils auprès du secteur privé. La question fondamentale de l'identité numérique est également évoquée et avec raison : comment avoir des systèmes d'authentification fiables qui favorisent les transactions à distance, sans tomber dans la paranoïa bigbrotherienne ? Le reste du rapport reste assez prévisible : formation, sensibilisation, recherche...
Tout cela est bel et bon et personne ne se plaindra de voir les administrations ou les entreprises dotées de meilleurs *firewalls* ou d'employés vigilants, attentifs à traquer les logiciels malicieux dans le moindre recoin de leur disque dur. Reste pourtant que tous ces efforts louables ne répondent pas à la question de fond : celle d'une doctrine stratégique.
Qu'est-ce qu'un acte de guerre informatique ? Quand faut-il pratiquer l'action préemptive, la riposte ou la dissuasion et contre qui ? Comment mesurer les effets d'attaques pour le moment surtout théoriques (quel que soit le volume du piratage informatique à finalité économique) et assurer la résilience des systèmes d'information ? Comment retransposer dans le cybermonde les règles de la menace, de la sanction ou de la négociation que connaissent les stratèges du monde réel ? Décidément les Américains ne sont guère plus avancés que nous stratégiquement et politiquement, même s'ils ont mis l'accent sur la technique.

17 février 2006 - Censure d'Internet en Chine
Yahoo, Google : capitalisme du virtuel et communisme bien réel

L'affaire n'est pas neuve. Les « ennemis d'Internet », entendez les gouvernements autoritaires, se sont toujours efforcés de contrôler la Toile, ou, du moins, d'empêcher leurs citoyens de recevoir des contenus subversifs de l'extérieur, de laisser filtrer de l'information gênante hors de leurs frontières et de créer des espaces numériques de discussion critique. Jusqu'à présent les experts pensaient que le parti de la censure perdrait forcément à long terme. Ils s'appuyaient sur plusieurs postulats qui se sont tous révélés faux :

- Internet était intrinsèquement porteur de liberté. Le développement des réseaux impliquait à la fois un accès potentiellement illimité à un information pluraliste et des possibilités de s'exprimer si vastes qu'elles seraient vite incontrôlables. La technique répandrait la liberté et seuls quelques esprits archaïques chercheraient vainement à freiner cette évolution inéluctable.

- Du reste développement des technologies de l'information et de la communication, développement économique par le libre jeu du marché et développement politique (entendez instauration d'une démocratie à l'occidentale) allaient de pair. Ce sens de l'histoire avait même un nom : c'était l'élargissement (enlargment), suivant le modèle global de la société de l'information. Ainsi, combler le fossé numérique contribuerait à répandre prospérité, esprit critique et valeurs démocratiques.

- Les États qui tenteraient de s'opposer au libre flux de la communication y parviendraient de moins en moins au fur et à mesure que leurs citoyens seraient mieux connectés, plus conscients et plus prospères. Face à cette résistance d'arrière-garde, l'esprit libertaire des internautes trouverait cent moyens nouveaux de ridiculiser les gendarmes de la Toile. Vouloir défendre un quelconque monopole de la pensée à l'intérieur de frontières nationales était une absurdité évidente à l'époque de la mondialisation et du village global.

Que nous enseigne l'exemple chinois ?

- Un État moderne peut concilier des taux de développement économique spectaculaires et une idéologie communiste. Il peut adopter les règles du marché, s'équiper de moyens modernes (avec plus de cent millions d'Internautes, la Chine est le second marché du monde après les USA) et ne pas changer son système politique. Or celui-ci repose en grande partie sur la domination des moyens de faire savoir et de faire croire

- L'État peut techniquement contrôler les flux d'information sur son territoire. Internet, contrairement à une idée reçue n'est pas un espace sans frontière. Bien sûr ce contrôle – comme tout contrôle de frontières – est loin d'être parfait. L'internaute astucieux peut contourner les obstacles, utiliser des sites dits « anonymiseurrs », ne pas se faire repérer par les autorités lors de ses navigations ou en utilisant certains termes interdits que repèrent les robots sémantiques... Mais la majorité des internautes chinois reste soumise à deux contraintes. Une contrainte policière : surveillance des cybercafés, obligation de faire connaître son identité pour toutes sortes d'opérations, traces laissées par les connexions… Une contrainte technique : pour aller sur Internet de Chine, il faut passer par un fournisseur d'accès sur le territoire chinois qui peut contrôler votre identité, vos connexions, les termes que vous employez dans vos mails ou sur votre blog et qui peut vous refuser l'accès à des sites interdits.

Ainsi, un serveur de messagerie qui est situé sur le territoire de la Chine est soumis à la fois à sa législation et à sa surveillance des contenus. Or toutes nos connexions et transactions sur Internet laisse une trace numérique. Par ailleurs pour s'informer sur la Toile, il faut savoir ou aller et pouvoir y accéder. Pour connaître l'adresse d'un site, il n'y a que trois méthodes. Soit quelqu'un vous l'a indiquée comme on fournit un numéro de téléphone, soit vous tombez sur le site en suivant un lien hypertexte, soit vous le repérez sur un moteur de recherche. Or le contrôle « autoritaire » sur la navigation exercé sur les navigations (les fournisseurs d'accès refusent de laisser l'internaute se connecter sur un site interdit) est renforcé par le contrôle « cognitif » des recherches. Si vous ne savez pas où aller chercher des images ou des textes interdits, vous ne risquez guère d'être atteint par eux. Le tout sur fond de contrôle linguistique : sa langue a toujours été une des meilleures défenses de la Chine contre les influences du monde extérieur.

Problème : comment empêcher un chinois d'aller chercher des contenus subversifs sur un moteur de recherche en chinois hors de Chine ? Réponse : en créant votre propre moteur de recherche sur le territoire national (Baidu) et en passant des accords avec Yahoo, Google ou Msn, alléchés par un gigantesque marché. Ainsi, les capitalistes yankees, si enclins à tenir un discours moderniste et libertaire ou à invoquer les droits de l'homme, se feront un plaisir de créer des moteurs de recherche locaux « bridés » suivant les demandes des autorités. , de« limiter » ces moteurs sémantiques et les portails, de fournir des techniques de surveillance, de traçage et de blocage d'accès, comme les milliers de « routeurs » de Cisco vendus à la Chine et qui repèrent les mots interdits. Ils pourront même transmettre les éléments pour inculper un dissident. Résultat : d'après Reporters Sans Frontières, il y aurait 49 cyberdissidents emprisonnés en Chine : un chiffre minuscule à l'échelle du pays, mais un signal fort.
Cerise sur le gâteau : les autorités de Pékin par la voix d'un responsable du Bureau d'Etat de l'Information, Liu Zhengrong peuvent se permettre de répondre aux Occidentaux : mais nous ne faisons que la même chose que vous ! Vous luttez contre les sites révisionnistes, terroristes ou pédophiles, nous protégeons nos citoyens contre la pornographie et la subversion.

Le sous-comité des relations internationales de la Chambre des Représentants a violemment pris à partie les sociétés US concernées à commencer par Yahoo (dont on dit qu'il aurait donné des informations permettant d'inculper deux de ses abonnés chinois) et Google (qui avait pourtant longtemps résisté à la pression de Pékin et avait même était « fermé » quelque temps en chine). Mais celles-ci répondent que c'est après tout au gouvernement US de régler le problème sur le plan diplomatique. Le pouvoir politique qui a adopté le Global Internet Freedom Act est-il désarmé face aux activités des entreprises privées hors de ses frontières ? Ce n'est pas certain. La législation sur l'exportation des technologies sensibles permet d'exercer une pression. Le Congrès pourrait imposer aux serveurs de messagerie de s'implanter hors des territoires d'États répressifs. Et il existe encore d'autres moyens.

Ils ont d'autant plus de chance d'être explorés que l'offensive contre la censure sur Internet est menée simultanément par des représentants démocrates et républicains également hostiles à la « Realpolitik » de compromission commerciale avec des régimes suspects.
Mais dans tous les cas, cette affaire nous aura rappelé une vérité : Internet est et reste un enjeu géopolitique. Que ce soit dans le domaine économique ou militaire, celui de la lutte contre le terrorisme ou celui de l'influence linguistique, idéologique et culturelle, c'est même un des

domaines les plus disputés.

Présentation du cours "Cybercrime, cyberguerre, cyberconflit"
dans le cadre du cycle annuel "criminalité" de l'IRIS

Qui a peur du " cybergeddon" ? Ce mot forgé à partir, d'une part de "cyber" (un préfixe qui signifie étymologiquement "gouvernail" et qui se retrouve dans des néologismes comme cybernétique, cyberespace, avec le sens de "lié à Internet") et, d'autre part d'Armageddon, la fin du monde. Alors, la fin du monde viendra du Net ?
La chose vous fait peut-être sourire, mais il semble que le FBI, s'exprimant par la bouche du directeur de sa " cyberdivision", y croie dur comme fer : "*les attaques sur des ordinateurs constituent le plus gros risque sur les perspectives de sécurité nationale. Elles sont des menaces pour nos infrastructures et notre intelligence, bien plus qu'on ne peut le croire*". Et d'expliquer, quelques jours après une simulation à l'échelon national et un rapport du très influent think tank CISIS, mettant Obama en garde contre la cyberguerre que le danger d'une attaque cyberterroriste pourrait être comparable à celui d'un nouveau onze septembre. D'une part des puissances étrangères, manipulant plus ou moins indirectement des groupes de hackers, tandis que, d'autre part, les terroristes prolifèreraient sur le Web 2.0. Et le tout pourrait être aussi dangereux qu'une attaque atomique ou que l'emploi des Armes de Destruction Massive (du reste, certains classent les "malwares", les logiciels malveillants parmi les ADM). Bien sûr, comme toutes les prophéties de malheur, celle-ci pourrait bien se révéler vraie un jour, mais, dans tous les cas, elle est tout sauf neuve.

Dès les années 90, voire avant, s'est développé une utopie d'Internet (agora électronique, possibilités d'expression pour tous, prospérité garantie par l'économie de l'immatériel, monde sans frontières, etc.), mais les dangers et fragilités de nos sociétés dépendantes de leurs systèmes d'information n'ont pas donné lieu à moins de projections terrifiantes.
Le « *Pearl Harbour informatique* », le hacker boutonneux paralysant d'énormes institutions avec un simple virus, le cyberespace livrés aux criminels ou aux pervers pédophilo-islamico-nazis, des cyberbrigades paralysant un pays entier en quelques secondes .., autant d'annonces récurrentes. L'hypothèse d'attaques informatiques a donc toujours été évoquée.
Et leur dangerosité a toujours semblé correspondre aux caractéristiques du numérique et des réseaux :
- la possibilité d'agir à distance, souvent anonymement, grâce à de simples algorithme, c'est-à-dire avec des « armes » qui sont en fait une connaissance transmissible d'attaquant à attaquant

- la valeur des biens immatériels devenus des données électroniques que quelqu'un peut altérer, reproduire, consulter, falsifier, capter, s'approprier, etc. à l'insu de leur propriétaire légitime
- les dégâts (en termes de chaos, perte de contrôle ou perte de biens ou de connaissances) que peut en principe produire une attaque contre des mémoires, des systèmes de transmission ou des systèmes de contrôle et de commandement
- la dépendance générale de nos sociétés de flots d'information en ligne
- l'accélération de la lutte de l'épée et du bouclier : moyens offensifs et moyens défensifs changent tous les jours : un nouveau logiciel malveillant peut apparaître demain, une nouvelle faille mais aussi un moyen de sécuriser
- la multiplication des acteurs susceptibles d'entrer en lice
- l'apparition de nouvelles stratégies étatiques, politiques, "privées" et intéressées visant à voler

des biens, à espionner, à saboter, à créer de la panique et du désordre (choses qui se font depuis toujours dans le cadre de crimes et de conflits), mais dans le cyberespace et par de nouveaux instruments numériques.

Ceux-ci évoluent sans cesse.
Orientées "attaque contre l'intégrité des systèmes" (par exemple les "dénis d'accès" menés par des *botnets* (des réseaux d'ordinateurs "zombies" dont on a pris le contrôle et que l'on peut "louer" à des attaquants), contre le contenu des mémoires ou des sites (visant par exemple leur éventuelle corruption pour diffuser des logiciels malveillants),
servant plutôt à prélever des données confidentielles, servant aussi à une fonction vitrine de proclamation et de communication (voire de défi symbolique), passant par les nouveaux outils du Web 2.0 dont les réseaux sociaux, utilisant le facteur humain (on parle de "social engineering" pour désigner de telles manipulations),
ces attaques sont diverses et évolutives.
Toutes posent des problèmes

- de capacité (purement technique et humaine),
- de traçabilité (qui est vraiment l'auteur d'une attaque qui est passée par de multiples intermédiaires ? comment le prouver ?),
- d'évaluation des dégâts
- et, bien sûr, de riposte (qui frapper, comment le dissuader ou le punir ?).

D'où la transposition dans le cybermonde des catégories du crime, du terrorisme et de la guerre

Le « cybercrime» est une appellation romantique de ce qu'il serait plus juste de nommer délinquance assistée par ordinateur (avec ses nouvelles formes). Des vols, des sabotages, des chantages, des escroqueries, des actes d'espionnage ou de viol de l'intimité, la diffusion de contenus illégaux…, tout cela peut être réalisé par écrans interposés.
S'y ajoutent différentes façons d'attaquer un système informatique (en pervertir le fonctionnement, en prendre la direction, y prélever des informations, ou encore le rendre inopérant).

À ce mot-valise - cybercrime - désignant une activité a priori intéressée, on associe volontiers guerre de l'information, mais aussi cyberterrorisme.
Le terme se réfère à des attentats qui s'exécuteraient sur la Toile par électrons interposés éventuellement contre des "infrastructures vitales". C'est une hypothèse agitée bien avant le 11 Septembre et qui ne s'est guère concrétisée hors quelques attaques informatiques contestataires bénignes et provisoires contre des sites officiels. La notion recouvre aussi l'utilisation des facilités d'Internet (communication à distance, anonymat, présence sur toute la planète…) par des groupes terroristes. Au total, ces deux curieux néologismes, faits avec un préfixe grec (cyber vient du mot qui signifie « gouvernail ») et des mots latins mal précisés (faudrait-il parler de crime pour tout ce qui se fait d'illégal sur Internet et dans le domaine informatique ? une activité qui ne fait pas de morts, par exemple l'envoi de courriels, mérite-t-elle vraiment d'être qualifiée de terroriste ?).

Enfin de récents événements (des attaques électroniques menées contre l'Estonie et dans une moindre mesure contre la Géorgie, des intrusions dans des systèmes informatiques attribuées à tort ou à raison à des grandes puissances) ont redonné quelque crédibilité à l'hypothèse

d'une cyberguerre. Celle-ci consisterait à préparer, relayer, amplifier et certains disent même peut-être remplacer, l'action des forces armées par des attaques électroniques contre des dispositifs militaires, étatiques (politiques ou administratifs) mais aussi privés. Par ailleurs, ces cyberattaques pouraient Le Livre Blanc de la Défense Nationale mentionne la "guerre informatique" parmi les problèmes de la sécurité nationale, insistant sur le fait que notre pays doit se doter de moyens de contre-offensive (et pas seulement de défense et de sécurité), ce qui suppose une doctrine d'emploi.

Le cours s'efforcera donc :
- de clarifier ces notions : comment, par exemple, transposer le concept de guerre qui suppose une violence létale, armée, collective, durable, publique et ostensible, visant un but politique (la "victoire") au monde des réseaux et des électrons ?
- de mesurer la distance entre les possibilités techniques de ravage et les stratégies qui peuvent effectivement y avoir recours : s'il est en principe possible de..., qui peut et désire pratiquement le faire, dans quel but et avec quelles conséquences ?
- d'évoquer quelques unes des contre-stratégies - pas seulement dans leur dimension technique, qui, par définition sera obsolète demain matin - mais dans leur dimension politique.

Pour compléter le cours, les étudiants pourront se référer aux documents suivant disponibles sur les site http://www.huyghe.fr :
Mythes et réalités des conflits dans le cybermonde : http://www.huyghe.fr/actu_628.htm
Guerre informatique et stratégie : http://www.huyghe.fr/actu_443.htm
Terrorisme, médias et communication : http://www.huyghe.fr/actu_227.htm
Le livre " Écran/ennemi" : http://www.huyghe.fr/actu_19.htm
Le livre "L'ennemi à l'ère numérique" : http://www.huyghe.fr/actu_524.htm