COLLÈGE DES
BERNARDINS

Chaire des Bernardins
2015-2017

L'Humain face au défi du Numérique

Séminaire du 7 décembre 2016
Intervenants : Stéphane TAILLAT

Compte-rendu : Maryvonne VALORSO-GRANDIN

Cyber Guerre - Cyber Paix
La conflictualité

Frédéric LOUZEAU

Bonsoir à tous et bienvenue pour cette séance. Avant de passer la parole à Milad Doueihi puis à Stéphane Taillat, puisqu'il y a beaucoup de nouveaux arrivants dans ces travaux de la Chaire des Bernardins *« L'humain au défi du numérique »*, je vais rappeler rapidement quel est notre programme général. C'est une Chaire d'études que nous avons lancée il y a maintenant presque deux ans. Elle est présidée par deux co-titulaires qui sont Milad Doueihi, philosophe et historien des religions, également président d'une Chaire d'humanisme numérique à l'université de la Sorbonne (COMUE), et puis Jacques-François Marchandise, directeur de la recherche et de la prospective à la Fondation Internet Nouvelle Génération (FING) que je dois excuser ce soir. Nous avons un Conseil scientifique présidé par Claudie Haigneré, que je remercie de sa présence ce soir.

La question que nous nous posons dans cette Chaire *« L'humain au défi du numérique »* est double :

- d'abord, qu'est-ce que le numérique fait à la vie humaine, à l'humanité, aux activités humaines ? C'est une question très vaste et donc on parcourt, depuis deux ans, différents domaines de l'activité humaine pour voir ce qu'il advient de ces activités dans le numérique, d'où aujourd'hui la question de la guerre ou plus exactement de la conflictualité ;

- ensuite, question plus redoutable et plus difficile sur laquelle nous aimerions bien progresser, est celle de savoir à quelles conditions sommes-nous capables, comme civilisation, d'habiter le numérique et de fonder un nouvel humanisme ? Comment pouvons-nous habiter ces environnements mais d'une manière qui soit humaine ?

Nous avons trois niveaux d'activité dans la Chaire :

- un premier niveau qui est un séminaire, sous deux formes : un séminaire comme celui d'aujourd'hui, plus ouvert, sous forme d'une cartographie de ces activités humaines et un séminaire sous forme de recherches, animé par Milad Doueihi avec lequel nous travaillons des grands textes philosophiques pour essayer d'appréhender cette transformation numérique ;

- un deuxième niveau appelé l'anti-séminaire : il s'agit d'ateliers de création numérique que nous avons créés l'an dernier pour des écoliers, des collégiens et des lycéens et, cette année, pour des étudiants, l'idée étant qu'il y ait un aller-retour entre une pratique du numérique et la réflexion des chercheurs ;

- un troisième niveau qui sont des évènements publics, organisés tous les six mois : le prochain doit avoir lieu le 23 février 2017 et s'appelle *« Numérique et diversités culturelles ».* Des chercheurs qui vont venir du monde entier, d'autres aires culturelles que l'aire européenne, réfléchissent aux mêmes questions que nous. Nous aurons donc un regard croisé.

Je vais passer maintenant la parole à Milad Doueihi qui va resituer notre réflexion d'aujourd'hui, sur *ce que le numérique fait à la guerre ou la conflictualité*, dans l'ensemble de nos recherches.

Milad DOUEIHI

Merci beaucoup Frédéric Louzeau. Je ne sais pas si je vais totalement répondre à ce qui m'est demandé, mais effectivement nous avions souhaité, en discutant entre nous et avec le Conseil scientifique de la Chaire, consacrer une séance au moins à cette question de la Cyber-guerre ou de la Cyber-paix devenue, depuis déjà quelques années mais plus récemment davantage encore, urgente et plus visible pour un large public. Quelque chose de cet ordre là est-il possible ? On y reviendra dans quelques instants, au cours de l'échange avec notre invité, mais auparavant j'aimerais essayer rapidement de mettre en perspective certaines des thématiques qui seront abordées par notre invité et dans la discussion, avec les sujets que nous avons déjà visités dans nos séminaires précédents ou nos autres activités.

Une des premières questions que nous nous sommes posées très tôt a été celle de la confiance et dans la dimension de cyber-guerre et de conflictualité, la conception d'une certaine confiance est essentielle et centrale, que ce soit du côté de l'Etat, des individus mais aussi du commerce, du modèle économique ou politique. On le voit bien aujourd'hui avec tout ce qu'on raconte sur le hacking des systèmes, en passant des machines électorales jusqu'à des dimensions plus stratégiques. On retrouvera donc certaines de nos réflexions sur la confiance qui, dans ce contexte très particulier de la cyber-conflictualité, subit des modifications. Je me rappelle très bien (j'imagine que certains d'entre vous s'en souviennent aussi, cela date d'une vingtaine d'années) des initiatives du Trusted Computing Group (TCG) visant à créer des systèmes d'exploitation très sécurisés et fiables. Aujourd'hui, avec le passage vers le réseau, le système est devenu moins important et toutes les modalités de construction de la confiance ont été transformées, comme on peut le voir à présent.

L'autre aspect que nous avons étudié et qui, d'une certaine façon, revient ce soir, concerne tout ce qui est de l'ordre de la trace, de la donnée et les façons dont celles-ci peuvent être exploitées, que ce soit pour des raisons économiques ou pour des raisons touchant à des aspects de la « privacy » ou à des questions de sécurité. Pour ne citer qu'un exemple de l'autre côté de l'Atlantique, j'évoquerai le hacking par les Chinois de toutes les données du personnel fédéral et d'une partie importante du gouvernement américain, pour se rendre compte très vite de l'échelle et de l'importance que cela peut prendre, ce qui élargit un peu le contexte dans lequel nous avions observé précédemment cet aspect.

Le troisième élément qui nous a beaucoup intéressés depuis le début de nos travaux, ce sont les liens qui ont pu exister depuis l'origine de l'informatique contemporaine, moderne, en tout cas des années 50 à aujourd'hui, entre le vivant et l'informatique, le vivant et la modélisation. Effectivement, beaucoup de modèles anciens reviennent aujourd'hui pour tenter de modéliser des systèmes de défense automatiques modelés sur le vivant, à l'exemple des cellules qui se défendent contre des éléments étrangers ou de l'introduction d'un agent extérieur dans le système vivant. On retrouvera aujourd'hui les questions que nous nous étions posées, mais dans le contexte très particulier d'un système d'agents relativement autonomes et façonnés sur le modèle du vivant.

Un autre élément également, sans doute plus complexe et qui nous intéresse plus dans les séances de recherche du séminaire, concerne toutes les questions soulevées aujourd'hui par la Cyber-sécurité ou la Cyber-paix sur lesquelles nous allons revenir, à savoir les conceptions que nous avons des notions de souveraineté, de territoires et de statut flottant des frontières lorsqu'on parle de Cyber-sécurité ou de Cyber-paix. Comment les déterminer ? Quels sont les éléments juridiques sur lesquels revenir, avec leur héritage théologique qui date pour certains de Saint Augustin, en passant par Saint Thomas d'Aquin, et avec toutes les théories de la guerre juste ou non ? Néanmoins, ces notions de frontières nous intéressent beaucoup car elles ont été transformées d'une certaine manière par le numérique et dans la Cyber-guerre, qu'elle soit défensive ou plus active du point de vue de l'attaque, se pose aussi la question de la cause juste et du cadre juridique lui permettant d'être légitime d'un point de vue national ou international.

Ceci nous amène à un autre élément concernant toute la question, émergente dans ce contexte, de la gouvernance. On trouve beaucoup de textes devenus aujourd'hui classiques, autour non plus simplement de la gouvernance de l'Internet telle que nous l'avions connue jusqu'à aujourd'hui, mais plutôt de formes de convention qui vont faire écho à d'autres formes de convention, que ce soit celle touchant aux Droits de l'Homme, ou à la Convention de Genève pour les prisonniers, etc. Quels seront les équivalents dans le cas de la Cyber-guerre et de la Cyber-paix ? Est-ce la voie à suivre ou bien faut-il proposer autre chose ? Et puis, autre élément qui m'intéresse d'ailleurs pour des raisons plus personnelles, c'est celui du vocabulaire souvent utilisé pour désigner certains objets exploités dans certaines attaques, comme par exemple les machines zombies. Il n'y a pas très longtemps aux Etats Unis, nous avons eu une attaque très importante où on a vu quelques millions de machines zombies, soit disant machines intelligentes, et on passe ainsi de l'intelligence au zombie en un instant, tout simplement parce qu'il y a une faille, un exploit connu même des producteurs qui n'ont pas eu la prudence ou la vigilance de le mettre à jour ou de le corriger et qui, *de facto,* peut générer des attaques.

Finalement, ceci m'amène à faire deux remarques. Tout d'abord, j'espère que nous pourrons revenir sur les éléments de la construction du statut juridique favorisant des formes non pas seulement d'attaque mais aussi de défense. On le voit très bien émerger aux Etats Unis, où un rapport vient d'être publié (il y a juste quatre jours) pour faire des

recommandations à la Présidence, parmi lesquelles on trouve la proposition de créer un poste d'Ambassadeur Cyber pour discuter et négocier ces sujets. Cela rejoint la question, vécue depuis toutes les fuites que nous avons connues, d'Edward Snowden jusqu'à aujourd'hui, du statut du secret diplomatique par rapport à la visée d'un idéal de transparence qui peut être souvent un moteur pour certains groupes hackers mais qui complique énormément certaines formes de négociation. Comment réfléchir à cette question qui nous fait sortir du cadre purement technique pour entrer dans des débats assez importants, mais récurrents puisqu'ils touchent à des notions de souveraineté, de secret d'Etat et ainsi de suite ? Ensuite, l'autre point tout aussi intéressant pour nous est le statut de la cryptologie aujourd'hui, en particulier du point de vue du droit au chiffrement ou non : doit-on avoir des « portes dérobées » comme on le dit en français, des *backdoors access,* c'est-à-dire la possibilité d'avoir ou non accès, d'autant que l'évolution technique semble promettre un changement important si on pense arriver un jour à quelque chose de l'ordre du quantique dans ce domaine. On commence à voir des premiers éléments qui peuvent complètement faire sauter le système actuel, ce qui donne matière à discussion.

Pour terminer, puisqu'on est dans ce lieu des Bernardins, je rappelle qu'on a toujours eu une certaine forme d'évangélisation, hier avec le numérique et aujourd'hui avec la Cyber-sécurité, en particulier côté Américain que je connais mieux, où on commence à voir apparaître des prophètes. Ce phénomène est assez intéressant à observer. Par contre, ce qu'on peut aussi observer, c'est qu'Il existe de plus en plus un écart entre d'un côté, le développement de la puissance du hacking et de l'autre, le déploiement de systèmes plus faciles à protéger. Cet écart, qui devient de plus en plus exponentiel, fait aujourd'hui problème. A mon avis, il renvoie à une question que nous avons déjà eue l'occasion d'évoquer, le fait qu'une des particularités, un des avantages du système de Cyber-sécurité, qu'on va étudier aujourd'hui, est de nous rappeler qu'on doit travailler sur le code et non pas exclusivement sur les usages ou les effets. A mon sens, le code est quelque chose à prendre très au sérieux. Je vais m'arrêter là pour remercier notre intervenant de sa présence et lui passer la parole.

Frédéric LOUZEAU

Auparavant, je vais présenter notre invité. Stéphane Taillat, merci beaucoup de vous être déplacé jusqu'à nous. Vous êtes professeur agrégé d'Histoire et vous enseignez aux élèves militaires de Saint-Cyr Coëtquidan. Vous êtes directeur adjoint du Mastère spécialisé *« Opérations et gestion de crise en Cyber-défense »* (responsable de l'axe *« Conduite des opérations »*) et co-auteur d'un livre *« Guerre et stratégie »* paru en avril 2015 aux éditions PUF. Vous avez la parole pour un long exposé puis un bon temps d'échanges avec notre public.

Stéphane TAILLAT

Bonsoir à tous. Je vais remercier le Père Frédéric Louzeau d'avoir fait appel à moi. C'est un sujet extrêmement délicat et je vais donc faire une première précaution qui est celle de dire qu'il y aura plein de lacunes dans ce que je vais dire. Je suis également chercheur au Centre de recherches des Ecoles à Coëtquidan et la particularité de ce sujet de Cyber-guerre, avec tous les thèmes parfois connexes ou parfois centraux que nous venons d'entendre, est qu'aujourd'hui les sciences sociales s'en sont parfaitement emparées, de manière très large, davantage peut-être de l'autre côté de l'Atlantique ou de l'autre côté de la Manche que chez nous, mais chez nous cela commence à venir aussi.

Donc, il y a forcément une diversité d'approches : le géographe, le sociologue, le politologue, l'historien vont s'associer. Nous-mêmes, nous travaillons avec nos collègues informaticiens pour essayer de comprendre ces phénomènes, évidemment, pour nous avec un tropisme qui est celui de notre fonction au sein des Armées : ce n'est pas qu'une fonction d'aide et de conseil mais c'est une fonction dans laquelle on apporte un maximum d'éléments de réflexion, si possible dans la formation bien entendu des futurs officiers de l'Armé de terre, mais aussi dans les cercles, au ministère de la Défense ou au ministère des Affaires étrangères. Donc, mon propos sera forcément lacunaire. Personnellement, je vais avoir un tropisme très relations internationales. J'ai une double formation d'historien et de politiste, donc il y a des points que je ne traiterai pas ou que je traiterai très rapidement et donc n'hésitez pas dans le débat à revenir sur des thèmes puisque je pourrai bien entendu vous répondre aussi sur d'autres éléments.

Peut-être, une autre précaution avant de commencer l'introduction, une introduction à l'introduction, un préambule. Vous avez remarqué que sur mon power point j'ai mis « Cyber-guerre ? », avec un point d'interrogation et des guillemets. Le terme lui-même est problématique. Je veux bien l'accepter par convention, utilisons-le par convention, même si je me souviens d'un séminaire à Ankara où on utilisait plutôt « *Cyber warfare* » qui me paraît plus pertinent, mais je vais expliquer pourquoi. Je vais donc l'utiliser par convention en disant tout de suite ce qui, à mon avis, est la bonne approche lorsqu'on veut traiter d'abord de cette notion de « guerre ».

Un court préambule donc pour dire que le problème du français est de n'avoir qu'un seul terme pour désigner une réalité complexe. On entend souvent le mot « guerre » de manière très restrictive, comme étant l'équivalent du combat. J'insisterai là-dessus dans l'introduction tout à l'heure. Ce n'est pas hors sujet de parler du combat lorsqu'on parle de la

guerre, mais on ne parle peut-être que de la pointe émergée de ce qu'est la guerre. Le combat est plutôt l'équivalent du *warfare* américain et je pense qu'il est important de restituer la guerre plutôt dans la conduite de la guerre, ou la tactique si vous préférez cette terminologie. Il est donc intéressant de se dire que le combat prend un sens, quelque chose lui donne son sens : c'est l'objectif que ce combat est sensé faciliter. Et puis, il y a autre chose qui donne sens à la guerre, ce sont les différents acteurs qui s'affrontent, c'est leur interaction, bref c'est la notion de stratégie.

J'insiste là-dessus et vous allez voir, tout de suite en introduction, en quoi *la Cyber-guerre aura-t-elle lieu ?* Je reprends ici, en le paraphrasant, le titre d'un article puis d'un ouvrage devenu extrêmement célèbre de Thomas Rid que j'ai l'honneur de connaître. C'est un chercheur Allemand, professeur aujourd'hui de Security Studies au King's College de Londres, qui avait fait paraître un ouvrage intitulé *« Cyber-war will not take place » (« La Cyber Guerre n'aura pas lieu »,* 2013), dans lequel il discutait justement cette notion de « guerre ». Pour simplifier, pour Thomas Rid, il est extrêmement problématique de parler de « Cyber-guerre », ce ne peut être qu'une métaphore. Pourquoi ? Parce que, selon lui, pour qu'on puisse parler de guerre, il faut que trois conditions soient remplies :

- la première condition est celle qui va s'apparenter au combat et celle que je vais traiter en premier dans cette introduction, c'est la létalité : pour qu'il y ait guerre, il faut qu'il y ait de la destruction et éventuellement même la mort,
- la deuxième condition est l'instrumentalité, c'est-à-dire que la guerre est un moyen, dont le combat est en quelque sorte, pour paraphraser Carl Von Clausewitz, la *« grammaire »,* mais il est loin d'en épuiser l'intégralité de l'essence même,
- la troisième condition est que la guerre est soumise à une logique, à des fins qui sont politiques.

Même si je ne suis pas entièrement d'accord avec lui sur ses conclusions, mais je n'en parlerai pas, je vais donc simplement développer ces trois points.

La notion de combat numérique : létalité, instrumentalité et fins politiques

Premier point, celui du combat. Peut-on vraiment parler de combat, c'est extrêmement problématique, quand on parle de Cyber-sécurité, de Cyberdéfense ? Peut-on en parler, que ce soit pour une entreprise qui protège ses réseaux, mais pourquoi pas aussi pour nous-mêmes ? Si nous protégeons nos données, nous voulons évoluer en sécurité sur Internet par exemple. Ou que ce soit bien entendu pour un Etat qui pense, à juste raison bien sûr, qu'il doit protéger un certain nombre d'infrastructures critiques, ou la stabilité de sa société, ou la survie du régime et tout ce que vous voulez ? Il est tout de même problématique d'aborder cette notion de « combat » parce qu'évidemment on ne voit pas se déployer, ou en tout cas pas de manière automatique et pas forcément de manière directe, la violence et la létalité.

Pourtant, et je vais utiliser l'expression de « combat numérique », on assume pleinement au ministère de la Défense cette notion : on parle bien de « combat numérique » et on renvoie bien à l'idée que le domaine numérique est en quelque sorte le lieu où s'affrontent des forces et où peut se déployer éventuellement de la violence. La particularité évidemment est que l'on sait, maintenant depuis relativement longtemps, que la force n'est pas forcément létale, que la violence peut être une violence psychologique, qu'elle peut être une violence physique. Je vais tout de suite, pour faire une transition avec le deuxième point, rappeler à la suite de Thomas Schelling qui écrivait cela dans les années 60-70, que : *la force, la violence ne servent pas avant tout à détruire, ne servent pas avant tout à anéantir ou à tuer, la force, la violence ont principalement des conséquences, des effets psychologiques, notamment en matière d'anticipation de la souffrance ou des dommages qu'elles peuvent créer*. Dans ce domaine là, il me semble donc pertinent de dire qu'il peut exister dans le domaine numérique le déploiement d'une telle forme de violence.

Mais, cela pose tout de même un deuxième problème quand on pense au numérique : c'est justement cet aspect instrumental. Est-on vraiment capable d'utiliser les outils numériques ? Est-on vraiment capable de manœuvrer, de se déployer dans l'environnement numérique ? De se déployer dans les réseaux de l'adversaire, ou dans les siens propres d'ailleurs, ou dans d'autres réseaux, de manière à pouvoir contrôler ce qu'on veut faire, de manière à pouvoir contrôler les effets de notre action ? Or tout de suite, dès qu'on pense au numérique, se pose le problème de la fameuse question de l'anonymat des attaquants, qui a souvent son contraire qui est la notion « d'attribution », c'est-à-dire la capacité d'imputer une action à un acteur. Notamment, si vous avez un peu suivi l'actualité, le hacking des emails de la Convention Nationale Démocrate (DNC) a été attribué, c'est-à-dire imputé, par le FBI (Federal Bureau of Investigation) et le Department of Homeland Security, à la Russie et évidemment on a vu immédiatement un certain nombre de personnes, des gens très versés dans l'aspect technique, ou des gens avec éventuellement une vision politique, qui calculent en termes de *qui a intérêt à faire cela ?,* dénoncer cette manœuvre d'attribution. *A minima*, leur argument consistait à dire, mais c'était aussi celui de la Russie pour s'en défendre, le Président Vladimir Poutine en premier : *mais, quelle preuve avez-vous que c'est moi ?*

D'où, la question qui se pose : le numérique peut-il être le vecteur qui permettra de faire pression sur un autre, de le dissuader éventuellement en lui montrant qu'on dispose d'un certain nombre de moyens, de capacités, ou de le contraindre à faire quelque chose ? Cela me paraît être une question importante : le numérique est-il un bon instrument ? Est-il un instrument fiable ? Si c'est un instrument fiable, on a des analogies dans l'Histoire militaire ou dans l'Histoire stratégique du 20e siècle qui montrent que des progrès ou des innovations technologiques sont vus comme de nouvelles armes « miracles », miracles en général pour l'attaquant et rarement pour le défenseur. Je fais référence à toute la littérature qu'il y a eue sur la puissance aérienne dans l'entre deux guerres, qui disait que la troisième dimension permettait de frapper les arrières de l'ennemi sur ses points faibles, sa population, ses usines et qu'on ne pouvait pas l'arrêter. Donc, il y avait l'idée que *voilà un instrument qui va permettre enfin de gagner les guerres*, comme si on pouvait gagner les guerres uniquement avec un moyen ! Même chose, à la fin des années 40 et au début des années 50, je pense en particulier à Bernard Bodrie sur *« Le nucléaire : l'arme absolue »* (1946), quand on a émis l'idée qu'on ne pouvait pas arrêter une frappe nucléaire ou que celle-ci était capable de désarmer définitivement l'adversaire.

Par conséquent, on a déjà eu dans l'histoire des moments où on s'est dit *on a une innovation technologique* et puis, un certain nombre d'autres éléments se présentent dans le contexte, comme le fait que nos sociétés soient extrêmement numérisées, que nos économies soient très numérisées, que notre système politique d'une certaine manière dans son fonctionnement soit également très numérisé, desquels découlent des vulnérabilités mais d'un autre côté, il y a un outil magnifique parce qu'on a toujours la possibilité de nier de façon plausible qu'on soit derrière l'attaque. Donc, on pense que c'est un bon instrument. Or je vous montrerai que ce n'est pas le cas : ce n'est pas un bon instrument ! C'est un instrument qui en fait se contrôle très, très mal ou qui ne peut être contrôlé que quand certains paramètres sont définis.

Parallèlement à cela, on observe pour la plupart des Etats depuis cinq-six ans, pour les Etats Unis c'est plus ancien, le développement de politiques que je vais appeler, de manière générique, de Cyber-défense, c'est-à-dire des politiques qui disent : *voyez, nous avons un domaine qui présente un enjeu qui n'est pas simplement de sécurité informatique mais qui est vraiment un enjeu de sécurité nationale.* Pour certains Etats qui ont vocation ou qui ont pour objectif de jouer un rôle sur la scène internationale, il peut même s'agir d'un enjeu de sécurité internationale, comme dans le cas par exemple, des Etats Unis qui estiment que la gouvernance de l'Internet est une question de souveraineté et ne voient pas que la gouvernance du numérique aille au-delà de la simple gouvernance d'Internet.

On a donc des politiques qui progressivement ont construit un enjeu de sécurité nationale, donc de niveau existentiel en présentant un certain nombre de menaces possibles et puis, il y a un certain nombre de crises qui semblent accompagner cette période. Sans remonter trop loin, on peut dire que le réveil pour tout le monde a été, en mai 2007, l'attaque majeure, par déni de service (denial of service attack), sur l'Estonie attribuée à la Russie ; en 2008, c'est le fait que cette même Russie, lors de sa guerre contre la Géorgie, ait aussi utilisé pour affaiblir son adversaire un certain nombre de moyens numériques, soit dans le domaine de la propagande, soit tout simplement dans le domaine du soutien et de l'appui de ses forces. Depuis, les crises se sont multipliées. Concernant les Américains, je rappelle que le 2 décembre dernier, le FSB, le Service de sécurité et de renseignement russe, déclare avoir empêché ce qui devait se dérouler ce lundi 5 décembre, à savoir une attaque générale contre le système bancaire russe. On ne sait pas évidemment quel crédit apporter à ces dires, mais les systèmes bancaires américains ont déjà été victimes de telles attaques, le groupe pétrolier Aramco basé en Arabie Saoudite a été aussi victime d'une attaque qui a effacé des données sur plus de trente milles ordinateurs, donc des actes qui ont de vrais impacts.

Partant de là, on se dit que, puisque ces crises existent, cela signifie qu'il y a des menaces et il est donc normal que les Etats aient défini le problème du numérique comme un enjeu de sécurité nationale ou internationale. Mais, n'est-ce pas en fait l'inverse ? Ne serait-ce pas plutôt, parce que les Etats ont progressivement défini le numérique comme un domaine ou un enjeu de sécurité nationale, qu'un certain nombre de crises sont devenues des crises ?

L'hypothèse, que je vais vous présenter et défendre, se décline en **trois points**, en sachant que ce sont des hypothèses probabilistes en contexte, c'est-à-dire que dans certains contextes elles seront plutôt vraies, alors que dans d'autres elles seront plutôt moins vraies et donc, je mets des guillemets :

- **la retenue stratégique**

La première idée que j'avancerai, encore plus vraie pour les acteurs non étatiques mais vraie aussi pour les Etats, est que l'objectif, lorsqu'on veut lancer une « Cyber attaque », est d'éviter les représailles. Pour cela, il y a un certain nombre de mesures à prendre et vous verrez que, loin d'être un milieu ou un domaine dans lequel l'attaque est avantagée, la défense a aussi son mot à dire.

Donc, la première conséquence est une tendance à la retenue stratégique, notamment de la part des Etats, c'est-à-dire la tendance à cibler, à viser surtout ce qu'on appelle des « cibles molles », c'est-à-dire des cibles soit qui ne peuvent pas se défendre, soit que l'attaquant estime, parfois à tort d'ailleurs, représenter un enjeu relativement faible pour sa victime. La tendance est de rester en dessous d'un certain seuil. Cela dessine donc plutôt, pour reprendre une analogie

avec l'époque de la Guerre froide, le paradoxe « stabilité/instabilité » : stabilité, car tout le monde sait que pendant la Guerre froide si on l'appelle la Guerre froide, c'est parce qu'il n'y a pas d'affrontement direct entre les deux Grands ; par contre, il y a des guerres périphériques dans lesquelles ils sont impliqués, parfois en dirigeant effectivement les opérations, d'autres fois en étant plutôt des opportunistes.

On retrouve donc ce paysage de stabilité/instabilité, ce qui veut dire qu'on aura un paysage sécuritaire marqué par une inflation des incidents, des attaques qui sont sérieuses pour ceux bien entendu qui sont touchés, notamment les entreprises et les individus, mais qui resteront, ou qui auront tendance ou qui pourront avoir tendance à rester en dessous du seuil où les dégâts seraient tels qu'ils nécessiteraient de la part de celui qui a été attaqué une réponse. C'est très important car, parallèlement, ce qui est en jeu est ce qui déterminera si oui, ou non, il existe un risque d'aggravation de tensions, d'aggravation de conflits, voire pourquoi pas de guerre ouverte entre deux acteurs à propos d'une attaque, d'une Cyber-attaque considérée comme majeure, et cela me semble être la variable indépendante.

- **la variable indépendante : la capacité de riposte de la victime**

Ceci m'amène à penser qu'il faut évidemment observer aussi de très près l'évolution du droit et en parallèle les débats juridiques, notamment la manière dont on va inscrire les attaques dans le domaine numérique dans le droit des conflits armés. Or, depuis quelques années, on a un manuel appelé le *« Manuel de Tallinn »* (2013), du nom de la ville d'Estonie où se trouve un Centre d'excellence de coopération de l'OTAN sur l'organisation de la Cyber-défense, qui a réuni des experts mandatés par l'OTAN sous la direction du juriste Américain Michael Schmitt et qui a clairement penché en faveur de l'application du droit des conflits armés et, globalement d'ailleurs, du droit international dans le Cyberespace. On retrouvera également dans la doctrine de dissuasion américaine, c'est-à-dire *comment dissuader des attaques numériques majeures*, l'idée qu'on se donne le droit de répondre sur tout un spectre. Depuis deux jours, c'est également le cas de la Russie, c'est aussi le cas en partie en France dans le *Livre Blanc sur la Défense et la Sécurité nationale* de 2013 où on retrouve cette notion que : *si on touche à nos intérêts vitaux, on pourrait éventuellement répondre au-delà simplement du domaine numérique.*

Donc, il faut contrebalancer cette tendance à la retenue stratégique avec le fait que justement on n'est pas toujours capable de calculer : on peut en effet se tromper sur la manière dont la victime va réagir. Sans doute que les hackers qui sont derrière le piratage et la divulgation d'un certain nombre de données confidentielles, mais aussi de la destruction d'autres données de la société Sony Pictures Entertainment en décembre 2014, ne s'attendaient pas (surtout si ce sont les Nord Coréens) à une réponse aussi ferme de la part du pouvoir Fédéral Américain lui-même. C'était la première fois que le Président des Etats Unis, le gouvernement fédéral Américain, attribuait une attaque, ce qui montre bien que c'est une variable extrêmement complexe.

- **La cause formelle : l'importance des représentations**

Ceci m'amène à la troisième hypothèse : l'importance de ce qu'on pourrait appeler une « cause formelle », quelque chose de l'ordre du structurel, à savoir l'importance des représentations. Lorsqu'on parle de Cyber-guerre, on touche en réalité l'un des deux récits, ou l'un des deux nœuds narratifs, qui courent depuis l'apparition ou le début de l'émergence du domaine numérique. Pour simplifier, en parlant par exemple d'Internet, vous voyez bien qu'il y a d'un côté, un récit narratif qui va plutôt insister sur le fait que c'est un espace de liberté, un espace même, pourquoi pas, d'émancipation, un espace d'opportunité, mais d'un autre côté, il y a toujours eu l'idée que c'était aussi un espace dont on pouvait éventuellement profiter pour accentuer une domination politique ou militaire, ou inversement un espace qui pouvait devenir un lieu de vulnérabilité et donc un vecteur d'attaque sur des réseaux critiques ou sensibles. Aujourd'hui, ce qui semble l'emporter ce n'est pas l'idée que finalement dans le Cyberespace, dans l'environnement numérique, ou même sur Internet, chacun peut gagner, les gains sont relatifs, on peut coopérer. Ceci reste encore bien entendu, mais ce qui semble l'emporter est plutôt l'idée que c'est un espace de conflictualité, dont la conséquence est la méfiance.

Je vais donc aborder notre sujet d'aujourd'hui **sous trois thèmes**, le domaine numérique comme enjeu de la conflictualité, puis le domaine numérique comme théâtre de la conflictualité et enfin le domaine numérique comme outil ou comme moyen de la conflictualité, en ayant bien en tête les trois hypothèses que je viens d'exprimer.

Le domaine numérique comme enjeu de la conflictualité

- **Premier enjeu : à numérisation croissante, vulnérabilité croissante**

La numérisation, ce phénomène d'échange d'informations sous forme numérique dans un monde de plus en plus croissant de domaines, semble ne pas connaître de limites aujourd'hui. C'est vrai pour Internet, ou pour l'accès à Internet, qui est aujourd'hui un phénomène quasi mondial, y compris dans les pays qu'on appelait autrefois en voie de développement, mais c'est vrai aussi dans les sociétés les plus développées ou dans les sociétés des pays émergents, puisque l'activité économique, l'activité sociale, l'activité culturelle, l'activité politique, l'activité bien sûr militaire sont aujourd'hui fortement numérisées.

Donc, la conclusion est : à numérisation croissante, vulnérabilité croissante. Pourquoi ? Parce que, on l'a dit tout à l'heure, il y a le code qui peut poser problème et être une première forme de vulnérabilité. Un de mes collègues, maître de Conférences en Informatique qui prône pour la formation des élèves officiers à Saint Cyr la notion de « programmation responsable », ne me démentirait pas : c'est très important de faire attention au code quand on programme quelque chose.

Mais, il y a d'autres vulnérabilités. Je vais citer ce qui semble être la plus importante aujourd'hui, même si peut-être effectivement il faut revenir au code comme première ligne de sécurité, à savoir la vulnérabilité liée aux comportements des individus ou des organisations. Et, à mon avis, les deux vont de pair car évidemment l'échange de données numériques par des ordinateurs est un mécanisme très déterministe, donc facile à tromper pour peu qu'on en ait les capacités techniques (bien sûr ce n'est pas mon cas), mais le fonctionnement des individus ou des organisations, qui ne sont pourtant pas déterministes mais qui peuvent être tout de même conditionnés par un certain nombre de procédures, ou d'habitudes ou de biais, peuvent aussi être faciles à tromper.

Pour paraphraser un chercheur de la Rand Corporation qui s'appelle Martin Libicky et a été un des premiers à s'intéresser à cette question : *il n'y a pas d'entrée forcée dans le Cyberespace.* Il veut dire par là que c'est un mur. Le réseau adverse est un mur dans lequel il suffit de trouver les failles qui existent déjà. C'est une vision peut-être un peu pessimiste, mais toujours est-il que plus la numérisation s'accroît, plus le sentiment de vulnérabilité s'accroît, avec tout de même cette précaution que la vulnérabilité n'est pas forcément équivalente à la notion de menace. Pour qu'il y ait une menace, il faut qu'il y ait un acteur malveillant qui souhaite exploiter cette vulnérabilité. Mais évidemment, je n'aurai certainement pas l'occasion d'y revenir, cela a beaucoup d'impact sur la structuration des politiques de Cyber-défense pour les Etats ou bien entendu sur les procédures de sécurisation des systèmes d'information pour les entreprises et pour les organisations. Peut-être faut-il en effet commencer par l'architecture du réseau ou du système, avant d'aller plus loin.

- **Deuxième enjeu : une structuration centre-périphérie**

Le deuxième enjeu important, cette fois-ci au niveau des relations internationales, est le fait que le Cyberespace, le domaine numérique, a beau être à la fois un espace global et transnational, à l'instar du reste des flux de la mondialisation, il est marqué par de très fortes inégalités, de très fortes différenciations, de très fortes disparités et plus précisément, pour reprendre un langage de géographe, par une structuration « centre-périphérie ». Cela signifie que l'accès à Internet est relativement aujourd'hui répandu à l'échelle globale, mais il existe encore des individus et des groupes qui n'ont pas encore accès à Internet soit pour des raisons techniques, soit pour des raisons socio-économiques, parfois aussi dans certains Etats pour des raisons politiques comme une forme de marginalisation. Tout ceci est vrai mais, si on s'en tient uniquement aux utilisateurs, aux gens qui participent à ce qu'on appelle la « couche cognitive » du Cyberespace, on a effectivement une impression de répartition très égale.

En revanche, si on prend les ressources qui permettent d'agir et de contrôler les flux d'information, ou de les détourner dans le Cyberespace, on voit qu'au contraire il y a une très forte disparité et une disparité entre les Etats et les autres types d'acteurs et puis, entre les Etats, il y a une disparité énorme. Soyons clair, entre les Etats Unis et le reste du monde la disparité n'est pas simplement due à leur rôle historique de créateur d'Internet mais est due aussi aux conséquences de la stratégie voulue en 1998, par l'administration Bill Clinton et par Al Gore à l'époque, de libéraliser Internet mais en encourageant les entreprises américaines à partir à l'assaut. Aujourd'hui, ce qu'on appelle les géants du Net, parfois on dit les GAFA (Google, Apple, Facebook, Amazon), sont évidemment Américains, ce qui explique en retour ce que j'appelle une lecture « hobbesienne » des relations internationales, c'est-à-dire une lecture dans laquelle les Etats qui se sentent exclus de ce système, ou qui pourraient se sentir menacés par cette domination américaine, ont tendance à réagir (ce qu'on ne leur reprochera pas) de manière qui pourrait aggraver les tensions sur d'autres domaines que simplement le domaine de l'économique, de la souveraineté numérique ou tout simplement de la souveraineté.

Donc à mon avis, cette structuration entrave pour le moment les capacités de coopération. Pour revenir à l'anecdote de tout à l'heure aux Etats Unis, où on parlait de souveraineté et de gouvernance, il y a eu un vrai dialogue de sourds entre la petite délégation française à laquelle j'appartenais et nos interlocuteurs américains, car visiblement nous ne parlons pas de la même chose lorsque nous parlons de « souveraineté » et de « gouvernance ». Mais, ce n'est pas étonnant parce que la souveraineté est elle-même un concept qui a des fondements à la fois juridiques et dans la philosophie politique, mais dont la pratique n'a jamais été fixe. Sur ce point particulier de l'Internet de la gouvernance du Cyberespace, très clairement nous utilisons les mêmes mots mais ils ne signifient pas la même chose pour les uns et les autres. Donc, il s'agit d'un enjeu important.

- **Troisième enjeu : les deux faces des politiques de Cyber-défense**

Cet enjeu, plus important encore par rapport à cette notion de guerre, c'est-à-dire par rapport aux potentialités de déclencher ou d'initier un conflit entre deux Etats, est ce que j'appelle les deux faces des politiques de Cyber-défense. Je vais introduire le concept, relativement connu en relations internationales ou en Security Studies, de « dilemme de

sécurité ». En quelques mots (ce concept étant très mécanique, selon les contextes il faut le faire varier), l'idée est que les Etats sont les seuls garants de leur propre sécurité et il existe, ce qu'on appelle en anglais « *come in Man-Trap* », c'est-à-dire le fait qu'un Etat aura beau affirmer que ses intentions sont de coopérer avec tout le monde, de faciliter la paix plutôt que la guerre, d'avoir bien entendu un appareil de défense mais uniquement défensif, ces protestations de bonne foi ne doivent pas, ou ne seront pas forcément prises à la lettre par les autres Etats, ses voisins naturellement ou ses rivaux, encore pire ses ennemis.

Le dilemme de sécurité découle donc de cette situation, ce qui signifie qu'un Etat qui veut être en sécurité est confronté à deux choix :

- soit, il démantèle son dispositif de défense, comme signe de bonne foi. C'est un peu extrême, mais il y a eu dans les années 70, en Scandinavie mais aussi en France, une réflexion sur ce qu'on appelait la NOD *« non offensive defense » (défense non-offensive*), c'est-à-dire l'idée qu'on pourrait concevoir des systèmes de défense qui, aux yeux de tout le monde, ne pourraient servir qu'à se défendre. Mais, c'est un piège parce que, dans cette situation là, l'Etat est comme s'il se désarmait, donc voulant être plus en sécurité en essayant d'affirmer sa bonne foi, il est plus en insécurité.

- soit, souvent il fait l'autre choix : pour être en sécurité, il va augmenter au maximum ce qui va garantir sa sécurité : ses alliances, son système de défense, pourquoi pas un petit coup de déstabilisation des potentiels rivaux et adversaires et pourquoi pas (ce sera très important pour le Cyberespace, on le sait grâce aux révélations d'Edward Snowden) s'introduire dans les réseaux des autres, ennemis, rivaux, mais éventuellement alliés, sans pour autant avoir d'intention néfaste mais parce que cela pourra toujours servir un jour. Sauf que cette approche-là, sensée garantir, augmenter la sécurité de l'Etat en question, va en fait aggraver sa sécurité par effets qui ressemblent à ceux de la course aux armements, c'est-à-dire par effets d'actions/réactions où les autres Etats vont à leur tour prendre ces intentions comme étant des intentions hostiles pour justifier de développer des dispositifs de défense qui pourraient éventuellement être utilisés de manière agressive.

Donc, on retrouve cette notion de « dilemme de sécurité » dans ces deux phases de politique de Cyberdéfense. Je rappelle que les « stratégies » de Cyber-défense ont trois composantes : une partie rhétorique dans laquelle on expose ce qu'on veut faire et en général on dit que c'est pour se défendre ; une partie opérationnelle bien entendu qui concerne la manière dont le dispositif est structuré pour remplir justement les objectifs ; une partie en termes de moyens, à partir desquelles, on peut juger ce que veut faire un Etat. Quand on regarde les différentes politiques de Cyberdéfense mises en œuvre par la plupart des Etats, ce sont des politiques qui :

- insistent sur la définition de ce qu'il faut défendre, ce qu'il faut protéger à tout prix,
- définissent des menaces, parfois de manière précise, parfois de manière très large, tous azimuts,
- et puis, en déduisent des dispositifs généralement de type « châteaux forts », ou parfois des dispositifs de résilience, qui sont deux manières de se défendre, en oubliant volontairement qu'il y a une troisième manière de se défendre : on ne se défend pas seulement en arrêtant l'attaque de l'adversaire sur la frontière, ou en étant capable de récupérer après une retraite stratégique, toujours en bon ordre bien entendu, on se défend aussi parfois en désarmant l'adversaire avant même que la guerre ne commence. Cela s'appelle la « guerre préventive », mais ce peut être aussi des Traités de désarmement ou de contrôle de désarmement.

Or, cet aspect est souvent éludé dans les politiques de Cyber-défense ce qui fait que, lorsqu'on les analyse, on voit bien qu'à chaque fois on dit : *on veut protéger nos infrastructures critiques !* Pour les uns, ce seront les réseaux, de ce qui assure la survie de l'économie de la société, c'est-à-dire les infrastructures de transports, les infrastructures énergétiques, les infrastructures de santé, bien entendu. Pour les autres, ce sera davantage ce qui assurera, à leurs yeux, la stabilité ou la cohésion de la société, *Information Security c*omme on le voit par exemple en Chine, ou ce qui facilitera la modernisation.

Mais, derrière ces déclarations-là, il me semble qu'il y a un non-dit : étant donné la nature particulière du domaine numérique, il consiste à penser que *ce n'est pas une option de ne pas faire appel à cette troisième modalité de la défense*, celle de se prémunir à l'avance en allant voir chez les autres, en s'introduisant dans leurs systèmes, d'autant plus que c'est très pratique : on parlait tout à l'heure de *backdoors*, la NSA (National Security Agency) est très forte pour ouvrir des « backdoors » un peu partout, sans aucun souci. Ce matin, le journal Le Monde a publié les révélations d'Edward Snowden sur le captage dans les avions, notamment Air France : il n'y a pas forcément d'intention malveillante, mais le problème est qu'on ne peut pas compter dessus, on ne peut pas compter sur la bonne foi, le fameux « *come in Man-Trap »*, qui fait que, sur un plan rationnel, les Etats peuvent coopérer pour éviter la conflictualité, mais que, dans la réalité, ils sont plutôt amenés à se méfier les uns des autres.

Le domaine numérique a tendance à renforcer ce cycle de méfiance qui va à son tour alimenter l'idée *qu'il faut tout de même aller voir chez les autres ce qui se passe.* Malheureusement, je suis toujours repéré à un moment ou à un autre, surtout si je suis Chinois ou Russe, moins si je suis Américain, car sans Edward Snowden il y a des choses qu'on ne saurait pas (les Américains ont l'air d'être un peu plus doués pour ne pas se faire repérer) et si je me fais repérer, cela alimente des tensions, surtout si ces tensions se rajoutent à d'autres contentieux éventuels ou d'autres raisons pour lesquelles je me méfie. La dernière doctrine Russe est très claire et s'inscrit d'ailleurs dans la doctrine de politique étrangère publiée la semaine dernière. Elle considère que les Etats Unis ne sont pas seulement un obstacle à la sécurité russe mais même à la stabilité du monde et donc, en matière de Cyber-sécurité, la nouvelle doctrine russe dit bien qu'il ne faut pas attendre que les Américains soient les premiers à frapper. Donc, vous voyez comment se crée un « dilemme de sécurité ».

Je vais conclure sur cet aspect « enjeux » en élucidant peut-être cette énigme. En réalité, quand on parle d'attaque et de défense, ou d'offensive et de défensive, on ne voit pas toujours que ceci doit être analysé à différentes échelles pour comprendre. Dans le combat, il y a un attaquant et un défenseur et on est successivement l'un et l'autre. A l'échelle d'un théâtre d'opération, on voit qu'il y en a un plutôt dans l'avance, l'autre plutôt dans la défense ou la retraite, mais il peut se préparer à contre attaquer. Donc, à ces deux niveaux là, le rôle d'attaquant et le rôle de défenseur ne sont pas aussi clairs qu'on pourrait le croire, et c'est là que le juriste, tout comme le politiste, ou le stratégiste doivent être attentifs, comme bien entendu le décideur politique, ou le décideur militaire, pour bien voir que le vrai niveau où se définissent les rôles d'attaquant et de défenseur se situe au niveau des objectifs.

Je vais prendre une analogie, si vous le voulez bien, avec ce qu'on appelle les « deux âges nucléaires » : l'âge nucléaire durant la Guerre froide et l'âge nucléaire aujourd'hui. Durant la Guerre froide, on est bien d'accord que l'arme nucléaire, en tout cas pour les Grands Etats, est une arme de dissuasion. C'est donc un dispositif défensif, préventif c'est-à-dire qu'on essaie d'empêcher l'autre d'agir, mais surtout on ne veut pas s'en servir. On a bien une arme offensive mais dans un dispositif défensif, dont on ne veut surtout pas se servir. Pourquoi ? Parce que l'objectif politique des Grands, pendant la Guerre froide, est la stabilité : c'est un objectif qui est par essence défensif. On veut essayer de maintenir un équilibre, on ne veut pas trop que le *statu quo* bouge. Le deuxième âge nucléaire qui est né à la fin de la Guerre froide montre qu'on peut très bien être un Etat qui se dote d'armes nucléaires, qui pratique la dissuasion, c'est-à-dire qui veut empêcher l'attaque des autres, mais à des fins offensives. Il va profiter du bouclier que lui fournit la dissuasion pour aller déstabiliser les voisins, augmenter sa place dans la hiérarchie internationale, etc.

Donc, on retrouve cette logique là dans le Cyberespace. Effectivement, il y a une forme de cycles d'instabilité à certains niveaux et l'objectif est d'atteindre entre les Etats le maximum de stabilité. Mais, ceci n'est possible que si les Etats en question ont des objectifs politiques défensifs, c'est-à-dire un objectif de conservation du *statu quo,* avec peut-être la volonté d'améliorer au moins leur situation. Mais, si ces Etats ont des objectifs de remise en cause de l'intégralité de l'ordre international, et ils peuvent avoir de leur point de vue des raisons valables de le faire sinon ils ne le feraient pas, alors en revanche c'est beaucoup plus embêtant pour la sécurité internationale.

Le domaine numérique comme théâtre de conflictualité

- **Autant de menaces et de pratiques que d'acteurs**

Le domaine numérique est un théâtre de conflit, avec un décalage entre les pratiques et les représentations. Je m'explique : quand on fait le décompte de tous les acteurs qui peuvent utiliser le Cyberespace pour atteindre leurs objectifs, que leurs objectifs soient des objectifs politiques (faire valoir leurs points de vues, déstabiliser l'adversaire, faire croire que les élections sont truquées, etc.) ou qu'ils poursuivent des objectifs économiques (tout ce qu'on appelle la Cybercriminalité, etc.), on voit bien qu'il y a une pluralité d'acteurs. Quand on essaie de mesurer l'impact de ces acteurs et des menaces qu'ils représentent, on est bien embêté : quels critères peut-on prendre ?

Si on prend le critère du coût économique, la catégorie d'acteurs qui a le plus d'impact est la Cybercriminalité : selon les chiffres, cela varie entre quatre cents millions et quatre mille milliards de dollars ! Donc, je ne m'amuserai pas à définir les critères des uns et des autres, mais en tout cas ce sont des sommes colossales. On estime que la Chine est un des Etats qui perd le plus à cause de la Cybercriminalité. Inversement, on sait en Russie traiter les Cybercriminels et les amener à s'intéresser à d'autres clients. Ce qui est intéressant est que, lorsqu'on regarde les politiques de Cyber-défense, ou la manière dont les Etats parlent des acteurs et des menaces, ils vont plutôt insister sur le Cyber Pearl-Harbor, côté Américain, c'est-à-dire le risque d'une attaque catastrophique : par exemple, les Chinois qui paralyseraient complètement l'infrastructure économique, politique voire militaire du pays et qui faciliteraient donc une attaque conventionnelle. C'est un scénario de science fiction, bien entendu ! Vous avez, bien sûr, tout ce qui concerne le risque de « Cyber-terrorisme », terme qui à mon avis ne signifie pas grand-chose, mais on voit l'idée que les acteurs, les organisations qui pratiquent le terrorisme comme une stratégie vont aussi investir le domaine numérique pour avancer, pour la propagande, etc.

Donc, il y a vraiment un écart entre les impacts réels et la manière dont on parle des menaces dans le domaine numérique. La plus grande menace dans le domaine numérique en fréquence est le fait que, vous et moi, nous nous retrouvions dans la situation où nos données bancaires, notre carte bancaire soient vendues sur le dark Web et il faut bien s'en protéger, parce que le lendemain on s'aperçoit que mille, trois milles, quatre milles euros qui ont disparu de nos comptes pour acheter quelque part, dans un super marché, en Californie ou ailleurs, peu importe. C'est une menace qui nous concerne directement. Bien sûr, il peut y avoir aussi des menaces liées à l'utilisation de nos données plus personnelles soit par des Etats peu scrupuleux, soit par d'autres types d'acteurs. Mais globalement, ce n'est pas cette menace là qu'on retrouve dans les documents, ce n'est pas elle qu'on retrouve dans les dispositifs. Ce qu'on voit le plus est le risque que l'Etat X ou Y, ou que l'organisation X ou Y, produise un effet décisif contre nous. Or, il y a peu de chances que cela se passe de cette manière là.

- **L'effet de « longue traîne »**

Dans le domaine numérique, il y a ce qu'on appelle un effet de « longue traîne ». Pour simplifier, par exemple Internet, et le Web 2.0 depuis maintenant seize ans, permet à n'importe qui de s'exprimer, permet une très forte mobilisation pour une cause (on va avoir plein de followers, plein de Likes pour dire : *il faut fait ceci, il faut faire cela)*, permet de diffuser de la propagande y compris dans les endroits les plus reculés où jamais elle ne serait arrivée avant, ou alors elle serait arrivée mais au péril de la vie des gens qui en l'occurrence font cette propagande, ou du moins au péril de leur liberté. Donc, le Cyberespace, l'environnement numérique permet l'expression de projets politiques extrêmement marginaux en termes de nombre de personnes touchées mais qui arrivent quand même à se parler les uns les autres et donc à exister.

C'est ce qu'on appelle l'effet « longue traine ». Or, c'est un effet qui a un revers et ce revers est le suivant : je vais prendre pour exemple, ce qu'on a appelé à une époque les « Révolutions 2.0 », c'est-à-dire l'idée selon laquelle on allait pouvoir, grâce à Twitter et aux réseaux sociaux, renverser des régimes politiques. Je fais remarquer que les Iraniens pensent que c'est une menace, les Russes certainement aussi, peut-être les Chinois aussi puisqu'ils parlent d'Internet comme du cheval de Troie des Etats Unis, mais quand on observe les cas concrets dans lesquels cela s'est passé, par exemple les révolutions Arabes, etc., on se rend compte que les « Révolutions 2.0 » n'existent pas. Certes, on peut mobiliser plus de monde, mais est-ce qu'on accroît la capacité d'implication individuelle des gens dans une lutte ? Certes, on va faire entendre son message à tout le monde, mais est-ce qu'on accroît la capacité de ce message à produire un effet sidérant sur toute une société ? Certes, on va avoir des organisations (c'est effectivement vrai pour des organisations non étatiques, par exemple djihadistes, capables de donner aux réseaux sociaux l'impression qu'ils sont encore vivants ou qu'ils sont en tout cas encore dangereux) capables d'augmenter une menace par rapport à la réalité de ce qu'elles peuvent vraiment faire, mais n'est-ce pas en fait à prendre avec énormément de précaution ?

En effet, comme je le disais, il y a besoin d'une inscription dans le réel : une action sur Twitter, c'est bien, mais une action politique dans la rue, c'est mieux ; de la propagande sur Internet, c'est bien, mais commettre un attentat en vrai (prenez-le dans le bon sens) est tout de même plus efficace. Ce que je veux dire, c'est que la capacité des réseaux sociaux, et cela a été très bien montré, va permettre d'organiser une opération égale à zéro, ou presque zéro, une opération qui tend vers zéro. Il y a un effet de résilience, ou effectivement de longue traîne, qui montre que beaucoup de gens, beaucoup d'acteurs sont apparemment dangereux, mais c'est aussi une illusion d'optique. Cette illusion d'optique nous rejoint aussi dans ce que j'appelle aussi un « jeu de dupes » à plusieurs niveaux.

- **Un jeu de dupes à plusieurs niveaux**

Là, je vais revenir à l'idée suivante : si je veux utiliser le domaine numérique comme le théâtre d'une opération, que ce soit par exemple, parce que je veux saboter, que je veux faire de la subversion, que je veux faire de l'espionnage, je vais être obligé de trouver les failles. La condition *sine qua non* pour que mon opération, qui ne se déroule pas à la vitesse de l'électron ou à la vitesse à laquelle je tape sur mon clavier, mais qui se déroule sur plusieurs mois voire plusieurs années, réussisse est la capacité à tromper les défenses de l'adversaire, et cela est encore plus vrai que dans d'autres types d'opération, ou dans d'autres théâtres, ou dans d'autres milieux.

J'ai parlé de « jeu de dupes » et donc la notion essentielle est celle de duperie, c'est-à-dire la capacité à simuler ou dissimuler les choses. Cette capacité est, à mon avis, un frein au fait de mener des opérations extrêmement ambitieuses, qui produiraient de vrais dégâts. Pourquoi ? Parce que cette capacité à tromper le réseau, les systèmes, les utilisateurs adverses est variable, d'autant plus si le système que je vise est considéré comme critique par ma cible et donc bien défendu, d'autant plus si je ne suis pas très sophistiqué d'un point de vue organisationnel. Certes, je vais d'abord faire une opération de reconnaissance et puis je vais essayer de m'introduire et je vais surveiller ce qui se passe, puis je vais essayer ensuite de produire un effet, etc., mais si je ne suis pas capable de découper en disant *untel, vous vous occupez du renseignement, untel vous vous occupez de ceci ou de cela, etc.*, si je ne suis pas capable de cloisonner, plus la cible représente un enjeu critique pour l'adversaire, moins je suis sophistiqué, comme c'est le cas pour les organisations non étatiques, plus ma capacité à duper sera faible. Pour illustrer, je vais prendre un exemple : on a fait des gorges chaudes parce que le soi-disant « Cyber-califat » a piraté le compte Twitter de l'US Central Command (CentCom), le

commandement de l'Armée américaine au Moyen Orient, en janvier 2015. L'effet psychologique de cette opération est sans commune mesure avec la réalité de ce qui s'est passé : ce qui a été attaqué n'a aucun intérêt stratégique, j'entends par là qu'il n'y avait aucune donnée confidentielle, le principal effet a été plutôt de faire croire qu'on avait fait quelque chose d'extraordinaire, alors qu'on n'a pas fait quelque chose de particulièrement compliqué.

Donc, ce jeu de dupes à plusieurs niveaux veut dire que, plutôt que d'envisager l'environnement numérique, le Cyberespace comme un seul espace homogène, il faudrait le découper en plusieurs sous-espaces. Vous auriez donc un espace où les cibles sont plutôt des « cibles molles », c'est-à-dire des cibles qui ne se défendent pas ou mal, ou qui ne sont pas du tout défendues, ou qui ne représentent qu'un enjeu faible et il est donc facile de les attaquer. Et puis, vous auriez un Cyberespace au dessus qui comprend tous les réseaux un peu critiques, bien défendus et alors là, pour les attaquer, bon courage parce que la probabilité de vous faire repérer est très importante. Donc, si vous voulez maintenir un niveau de duperie, de tromperie de façon à ce qu'il garantisse votre sécurité opérationnelle, la sécurité de votre opération, il faut y aller doucement, sur des petites cibles, éventuellement en s'attaquant à des systèmes qui soient à la marge, mais pas au cœur du réseau de l'adversaire.

Le domaine numérique comme moyen, outil de la conflictualité

Ceci m'amène à dire qu'il faut un peu contextualiser lorsqu'on s'intéresse à ce panorama de la Cyber-guerre, de la Cyber-sécurité, de la Cyber-conflictualité.

- **L'état de la numérisation**

En réalité, l'état de numérisation, c'est-à-dire le degré de numérisation des sociétés ou des acteurs et leur degré de sophistication organisationnelle, est très inégal. On ne peut pas comparer la Russie, la Chine, ou les Etats Unis avec l'organisation Etat Islamique par exemple, dans ce domaine. L'organisation de l'Etat Islamique est bonne, ses gens savent faire un certain nombre de choses, mais ils n'ont pas le niveau de la NSA. Le GRU (le renseignement militaire russe) est un peu en dessous parce que visiblement il ne s'est pas entendu avec ses collègues du FSB, ensuite il y a des problématiques bien connues en sociologie des organisations, des problématiques souvent de rivalités bureaucratiques. Je pense que nous-mêmes, nous ne sommes pas mauvais. Mais, si on veut vraiment s'intéresser à *qui est capable*, ou *qui va être tenté,* d'utiliser le Cyberespace pour produire des effets qui auront vraiment un impact, celui d'atteindre les objectifs, il faut regarder du côté des Etats, et des Etats les plus puissants, ce qui ne veut pas dire qu'il ne faut pas regarder les autres, parce que ce sont peut-être des nuisances, mais ce sont des nuisances qui pour les gens qu'on veut protéger, donc en termes de légitimité politique, de souveraineté du fait que l'Etat est garant de la sécurité, sont importantes.

- **L'intégration différenciée**

Le numérique est intégré aujourd'hui dans les moyens traditionnels de la défense, de la guerre. Autrement dit, il existe aujourd'hui, de plus en plus, un mouvement dans lequel on va intégrer les « capacités Cyber », comme on les appelle. Il y a eu, dans les dix dernières années, des exemples historiques qui ont montré qu'on était capable d'utiliser les armes numériques comme des soutiens, des appuis à des opérations conventionnelles. J'ai déjà cité tout à l'heure la Russie qui a fait du « défacement », on sait aussi qu'en Ukraine ils ont contribué à semer la pagaille en coupant un certain nombre de centrales électriques, etc., mais je vais citer deux autres cas :

- A tout seigneur tout honneur, je vais d'abord citer l'exemple des Américains : en 2007-2008 pour lutter contre Al-Quaïda en Irak, lors de cette grande campagne qu'on a appelée le Surch, les Américains se sont servis du fait qu'en face d'eux, les insurgés avaient aussi des téléphones portables, étaient connectés à Internet, et donc qu'on pouvait faire de la manipulation, recueillir des données, tromper l'adversaire et qu'on peut capitaliser sur cela pour d'une part, accélérer la « destruction » de l'organisation ennemie et d'autre part, paralyser, obliger l'organisation insurgée, ses chefs, ou certaines cibles à privilégier leur protection, leur sécurité plutôt qu'à monter de nouvelles opérations. C'est un exemple qui est aujourd'hui bien documenté.

- Je vais citer ensuite l'exemple des Israéliens et l'opération Orchard qui a eu lieu en septembre 2007 : grâce à une clé USB laissée de manière imprudente sur un ordinateur, le Service de renseignement israélien a découvert que les Syriens étaient en train de construire, ou avaient pour projet de construire une centrale nucléaire à Deir ez-Zor et donc la décision avait été prise, à l'habitude des Israéliens, de faire en sorte que cette centrale ne voit jamais le jour. Il s'agissait de frapper par un raid aérien, un peu comme ce qui s'était passé à Osirak en Irak dans les années 80, sauf que la défense aérienne syrienne est quand même sérieuse, et donc il faut qu'au minimum cela se passe vite, ce n'est pas vraiment du clandestin parce qu'on saura que ce sont les Israéliens, mais il faut que cela se passe vite. Et donc, les Israéliens ont utilisé des malwares pour rendre aveugles, tromper les radars de la défense aérienne syrienne, un peu comme Stuxnet avait trompé non seulement les systèmes de contrôle des centrifugeuses de Natanz, mais même aussi tout le monde.

Donc, aujourd'hui, c'est une réalité et en cas de conflit ouvert, on peut imaginer sinon une Cyber-guerre mais des forces qui utiliseront le numérique soit comme talon d'Achille pour frapper quelqu'un, soit comme « multiplicateur » de forces, mais toujours en appui et non pas comme étant une arme principale.

- **La notion de Cyber-armes**

J'en viens donc à parler de cette fameuse notion de « Cyber-armes », qu'on entend parfois. D'ailleurs, il est parfois question, cela avait été demandé en 2011 par exemple par les pays de l'Organisation de coopération de Shanghai (OCS), d'avoir une espèce de désarmement « Cyber » ciblant, bien entendu, les Américains. On sait qu'il existe un marché de ce qu'on appelle les « exploits Zero-Day », etc. Il y a effectivement des outils qui s'apparentent à des armes.

Pour reprendre une des réflexions de Thomas Rid dans *« Cyber-war will not take place »,* dans lequel il explique, en prenant une image, qu'en fait si on veut essayer de comprendre la notion de « Cyber armes », il faut les placer en quelque sorte sur un continuum. Il dit que d'un côté, il y a le pistolet de Paintball et de l'autre, il y a la bombe à guidage laser, pour nous montrer qu'en réalité il y a toute une catégorie de malwares. L'immense majorité des malwares reste plutôt du premier côté du continuum, du spectre, c'est-à-dire que ce sont plutôt des armes qui vont être très peu discriminées, c'est-à-dire qu'en général elles peuvent cibler par exemple cet ordinateur comme n'importe quel ordinateur. Mais, cela peut d'ailleurs être assez dangereux de les utiliser parce que cela peut vous revenir comme un boomerang mais, surtout, parce que ce ne sont pas des agents intelligents.

On parlait tout à l'heure, d'autonomisation de la défense, mais la vraie question est aussi en attaque : pour pouvoir réussir sa manœuvre de duperie/tromperie des réseaux adversaires, il vaut mieux avoir des agents intelligents. Donc, la plupart de ce qu'on trouve dans le commerce ou sur le marché, ce sont ces outils là. Ils ont leur intérêt, une bonne veille attaque de déni de service, c'est-à-dire une attaque brute qui va mettre par terre des sites Internet ou des réseaux peut se révéler très pratique pour appuyer, pour faire du *signaling,* pour montrer qu'on menace, ou peu importe, mais globalement les malwares entrent plutôt dans cette catégorie en grande majorité d'armes qui sont très indiscriminées et qui ne sont pas des agents intelligents.

Et puis, il y a la petite pointe, celle des agents intelligents dont Stuxnet est certainement l'exemple ultime. D'ailleurs, Stuxnet est capable de s'adapter pour discriminer, cibler et il était programmé pour ne se déclencher que sur des systèmes d'exploitation bien spécifiques, ou des configurations matérielles et logicielles bien spécifiques, ce qui veut dire que n'importe qui ne peut pas s'en servir : il faut avoir de vrais agents de renseignements sur le terrain, comme celui du Mossad par exemple, pour savoir quelles sont ses configurations matérielles et logicielles. On a donc là un petit arsenal, qui ne sert qu'une fois, même si le code Stuxnet s'est retrouvé disséqué un peu partout après, il est difficile de le réutiliser tel quel, il va falloir le réadapter.

- **Les opérations clandestines**

Tout ceci m'amène au point de savoir comment replacer les opérations numériques ou les armes numériques dans la stratégie à l'échelle internationale ? Ce n'est pas moi qui le dit, c'est une conclusion à laquelle beaucoup de chercheurs aujourd'hui, et de praticiens d'ailleurs aussi, sont arrivés : on est plutôt dans le domaine des opérations clandestines, c'est-à-dire que les armes numériques sont très utiles pour faire des opérations clandestines, des opérations de renseignements, des opérations dans lesquelles, même si la victime sait que c'est vous, vous aurez toujours la possibilité auprès d'autres auditoires de dire *non pas du tout, vous n'avez aucune preuve*, des opérations dans lesquelles on cherchera à faire du sabotage, de la subversion, de l'espionnage pour reprendre, là aussi, les trois catégories de Thomas Rid. Ces opérations sont donc très utiles mais il arrive rarement que les opérations clandestines renversent le cours d'une guerre, que des opérations clandestines modifient durablement l'équilibre des pouvoirs, ou les rapports de force entre les Etats sur la scène internationale. Cela peut arriver, mais sur un malentendu, c'est-à-dire que ce sont des opérations où, normalement, on essaie de contrôler un effet directement, mais ensuite on ne sait pas ce qui va se passer. Ce principe est encore plus renforcé dans le domaine numérique puisque, dans le domaine numérique, calculer exactement quelles vont être les conséquences de vos actes, de vos attaques, est extrêmement compliqué : il y a ce que vous voulez faire, vous allez éventuellement pouvoir le faire, mais il y a à côté tout ce que vous n'avez pas voulu faire qui risque de déborder. Donc, les armes numériques sont plus utiles pour les opérations clandestines qu'elles ne sont des outils de dissuasion ou de coercition.

Aujourd'hui, on voit bien que se faire entre deux Etats la guerre de manière frontale est, pour plein de raisons que je n'ai pas le temps d'expliquer, très compliqué. C'est même hautement improbable. Aujourd'hui, la guerre entre les Etats est hautement improbable, sauf malentendu et j'y reviendrai. Par contre, les Etats continuent à être en rivalité, y compris d'ailleurs parfois entre amis, ils continuent à avoir des compétitions musclées ou à être en désaccord très, très fort sur certains sujets. L'idée est : *comment je vais faire en sorte que l'autre cède ?* L'objectif maximal est évidemment qu'il cède sur toute la ligne, mais je sais que plus probablement je n'utilise pas la force de manière directe, que plus probablement il va céder un peu et puis moi aussi et finalement je serai obligé de céder.

Donc aujourd'hui, la force militaire (je ne parle pas du numérique mais de la force en général) sert essentiellement à influer ce rapport là, soit par de la coercition, c'est-à-dire je vais essayer de contraindre l'autre à céder, soit par de la dissuasion, c'est-à-dire je vais essayer de l'empêcher de manœuvrer de telle ou telle manière pour me coincer. La force militaire, aujourd'hui plus que jamais, contribue à la diplomatie. On retombe presque, et je vais citer Frédéric Legrand au 18e siècle, *la diplomatie sans armes c'est comme la musique sans les instruments*, dans une forme de complémentarité entre la force militaire et les autres outils de la politique étrangère. Après, il faut savoir bien les combiner, ce qui est encore une autre affaire, surtout si en face on a des adversaires qui réfléchissent, bien entendu.

Il me semble que le numérique n'est pas du tout fait pour cela. Comme instrument de coercition, il suffit de regarder l'exemple de l'Estonie : si les Russes avouent que ce sont eux qui sont derrière l'attaque de déni de service, dans ce cas là, ce qu'avait demandé à l'époque l'Estonie, à savoir invoquer l'article 5 du Traité de Washington de l'Otan pour appeler les autres à son secours, cela va se passer très mal pour la Russie parce que, même si les autres alliés ont estimé que c'était un peu exagéré d'invoquer l'article 5, le dispositif de l'Otan précisément s'est tout de même reconfiguré. Donc, si la Russie le dit, « avoue », cela risque bien entendu d'être négatif pour elle. Mais, si la Russie ne dit rien, le flou subsiste car on ne sait pas quelle est l'intention de l'attaquant et donc pourquoi lui céderait-on ? Pourquoi est-ce qu'on céderait à la demande de la Russie de laisser en place cette statue du soldat russe qui commémore la fin de la Seconde Guerre mondiale, mais qui aux yeux des Estoniens commémorait plutôt les cinquante ans de présence soviétique qui avaient suivi ? Donc comme instrument de coercition, ce n'est pas l'idéal.

En conclusion,

- **Le domaine numérique rajoute de la complexité**.

Le domaine numérique rajoute de la complexité. Il ne faut pas le nier, mais aujourd'hui on a pris conscience en France, mais dans de plus en plus d'autres Etats qu'il faut former des gens pas simplement aux aspects techniques du numérique mais aussi aux aspects opératifs, c'est-à-dire à la combinaison de l'ensemble des moyens et voire même, aux aspects politico-stratégiques, c'est-à-dire pour qu'ils soient capables d'expliquer aux chefs qui vont prendre les décisions et même aux dirigeants ce qu'il en est (là, je fais de la publicité pour notre Mastère spécialisé qui est réservé à un certain nombre de personnes, mais c'est notre idée de travailler ces aspects). Cela rajoute de la complexité mais au fond cela ne révolutionne pas les relations politico-militaires. Vous verrez qu'ensuite je vais prendre ce point là avec une certaine prudence.

- **Attention aux analogies avec le nucléaire**

Ensuite, attention aux analogies avec le nucléaire. J'en ai déjà parlé tout à l'heure, mais on a pendant très longtemps, jusqu'à quelques deux-trois ans, dit que : *le Cyber c'est finalement comme le nucléaire et donc, il faut faire de la dissuasion comme à l'époque du nucléaire*. Depuis, on s'est rendu compte que la dissuasion nucléaire est une dissuasion absolue, ce qui signifie qu'à partir du moment où l'autre utilise ses armes contre vous, c'est que vous avez échoué, c'est fini ! C'est pour cela que dans notre doctrine on parle de re-crédibiliser éventuellement la dissuasion en frappant, une frappe limitée, pour rappeler qu'on est sérieux quand on menace un potentiel agresseur de représailles nucléaires. Mais globalement, l'idée est de dire : si *l'autre agit, c'est que la dissuasion a échoué*.

Mais dans le monde qui est le nôtre depuis 1990, face aux menaces auxquelles nous sommes confrontés, on voit bien qu'on ne peut pas empêcher que des attaques aient lieu, on ne peut pas empêcher réellement que des attentats se produisent (on ne peut pas empêcher tout attentat), on ne peut pas empêcher toute attaque numérique. Donc, la dissuasion ne peut pas fonctionner comme la dissuasion nucléaire, elle ne peut qu'apporter quelque chose de plus pour essayer de limiter le nombre d'attaques ou le nombre d'agressions. Il y a des moments où les attaques passeront à travers les mailles du filet. Qu'est-ce qu'on peut faire ? Est-on capable à l'avance de modeler l'adversaire, comme le font les Israéliens mais pas toujours avec succès, c'est-à-dire expliquer à coups de bombes qu'il y a des choses qui se font et d'autres qui ne se font pas ? Ou à l'inverse, est-on capable de faire de la résilience, c'est-à-dire que même à mal, on arrive à se reconstruire (je schématise, bien entendu) ? Donc, l'analogie avec le nucléaire n'est pas bonne. L'analogie avec la puissance aérienne, non plus.

- **Le bel avenir de la Défense**

En corollaire de ce que je viens d'expliquer, on a trop longtemps expliqué (notamment dans la littérature américaine au moins jusque dans les cinq dernières années) que le domaine numérique était celui où allaient avoir lieu des attaques catastrophiques contre lesquelles on ne pourrait pas se prémunir, parce que d'un côté, on montrait qu'on était très numérisé, donc très vulnérable, et de l'autre côté, qu'il y avait toujours des failles, ce qui sous entend évidemment que l'attaque catastrophique est derrière. Je parlais de « Cyber-Pearl Harbor » tout à l'heure, il s'agit d'une expression utilisée deux fois, en 2010 et en 2011, par le Secrétaire américain à la Défense, Leon Panetta, qui a créé la première doctrine de Cyber-sécurité américaine.

Or en fait, je voudrais dire qu'au contraire le Cyber, le numérique, au moins par rapport à des attaques numériques, favorise plutôt la défense, pour la raison que j'ai expliquée tout à l'heure, c'est-à-dire pas pour nous, pauvres individus, pas pour les entreprises malheureusement, quoique l'Etat peut choisir, comme en France et comme aussi en Grande Bretagne depuis l'automne (les Britanniques se sont rendus compte, alors qu'ils voulaient laisser la sécurité des entreprises à elles mêmes en leur donnant de l'argent, que cela ne marchait pas), de chercher à prendre en compte, à garantir la sécurité de ce qu'on estime être des opérateurs d'intérêt ou d'importance vitale.

En dessous de cette sphère, donc au cœur de nos systèmes de défense militaire, ensuite nos systèmes qui font fonctionner l'Etat, ensuite les systèmes qui font fonctionner la société et l'économie, au-delà de ces cercles là, il y aura effectivement des attaques et l'attaquant aura l'avantage parce qu'on a des cibles mal défendues, ou pas défendues, ou parce que ce sont des enjeux relativement mineurs, même si on peut toujours se tromper. Par contre, dans ce système que je viens de définir, il y a de fortes chances qu'un attaquant, même très sophistiqué, y regarde à deux fois. Pourquoi ? Parce que le risque pour lui est de se faire découvrir et se faisant découvrir, étant données les doctrines de défense qui se mettent en place progressivement, il sait qu'il peut craindre un retour de bâton.

- **Les risques d'escalade**

Donc en fait, le vrai problème n'est pas tant une guerre numérique mais une guerre à propos du numérique, c'est le risque d'escalade. Que se passe-t-il demain (imaginons un scénario réel, mais un peu modifié) si Barak Obama en décembre 2014, lorsqu'il attribue l'attaque de Sony Pictures Entertainment à la Corée du Nord, parce qu'il doit montrer au Congrès qui n'arrête pas de le critiquer qu'il est ferme sur cette question, ou qu'il doit rassurer le Cyber Command ou la NSA sur sa volonté de leur laisser les mains libres sur un certain nombre de choses, ou parce qu'il craint au contraire qu'une réponse uniquement dans le domaine numérique à cette attaque dévoilerait des capacités de la NSA, ce qui ne serait pas bon, décide des représailles militaires sur la Corée du Nord ? C'est hypothétique, mais pas tant que cela, on a déjà vu des présidents Américains qui ont eu parfois la gâchette facile lorsqu'il s'agissait de répondre (de leur point de vue, c'était logique d'ailleurs) par exemple, à un attentat par une frappe militaire. Je rappelle le raid sur Tripoli en 1986 par exemple.

Il y a une tendance à la retenue stratégique : les acteurs qui sont les plus capables de faire mal, c'est-à-dire les Etats, ont intérêt, aujourd'hui c'est ce qu'on observe, à se retenir et à ne pas chercher à frapper les systèmes jugés critiques, jugés importants par leur cible, parce qu'ils ne sont pas garantis, loin de là, qu'ils ne soient pas découverts et qu'il n'y ait pas des représailles derrière. Le problème est que, comme dans la doctrine de dissuasion nucléaire, il y a un seuil. Ce seuil, dans une bonne doctrine de dissuasion nucléaire, à base de représailles militaires, on dit qu'il y en a un mais on évite de le fixer de façon précise pour éviter que l'agresseur sache à quel niveau le situer.

Dans le numérique, dans le Cyber, c'est exactement la même chose. Aujourd'hui, le risque est que la plupart des Etats considèrent, parce que ce sont des enjeux de sécurité nationale ou que cela s'inscrit en plus dans des tensions croissantes entre certains Etats (entre Russie et Etats Unis par exemple), qu'une attaque touchant leurs intérêts vitaux, que ce soit des intérêts matériels ou des intérêts symboliques, pourrait donner lieu à une réponse bien sûr juridique mais pourquoi pas militaire. Pour ces raisons, un risque de mauvais calcul de la part d'un agresseur n'est pas à exclure. Or aujourd'hui, nous nous trouvons (je ne parle pas de la Chine parce qu'elle n'est pas dans cette logique là, mais depuis trois ans la Russie semble l'être) en Russie face à un Etat qui tend progressivement à ce qu'on appelle, en relations internationales, un Etat révisionniste, c'est-à-dire un Etat qui n'est pas content du système actuel (de son point de vue, évidemment c'est tout à fait logique) et qui veut le réviser. Le problème, l'Histoire nous l'apprend, est qu'il y a deux manières de réviser l'ordre international lorsqu'on en est mécontent : la première est d'essayer de jouer les règles et de les redéfinir à son avantage pour progressivement prendre une place importante au cœur du système ; la deuxième est d'essayer d'affronter directement, face à face, le tenant du titre. Mais ensuite, il y a évidemment une troisième solution : le tenant du titre voit venir l'attaque et frappe le premier.

Dans ce contexte là (j'ai beaucoup suivi les élections américaines, mais aussi les affaires liées aux questions nous concernant ce soir), le plus inquiétant n'est pas ce que les Russes font, mais c'est la combinaison entre ce que les Russes font et la manière dont c'est reçu aux Etats Unis par les élites politiques et militaires. Evidemment, je ne suis pas un prophète et je ne le souhaite pas, mais la combinaison entre les deux me paraît bien illustrer ce que j'appelle les risques d'escalade, c'est-à-dire comment, à propos d'une attaque numérique, il pourrait y avoir un affrontement, peut-être pas tout de suite un affrontement armé, mais en tout cas un accroissement des tensions sur la scène internationale. Voilà, j'ai beaucoup parlé, je ne suis pas sûr d'avoir été toujours clair, mais je serai très heureux de répondre à vos questions. Merci de votre attention.

Milad DOUEIHI

Merci beaucoup. Juste quelques mots avant de passer la parole à la salle, en réaction à votre dernière remarque sur les actions russes et les réactions américaines, je voudrais apporter un point de vue de l'autre côté de l'Atlantique. A mon

avis, ce qui est plutôt rassurant c'est que les Américains et les Russes retrouvent finalement un jeu qu'ils affectionnent beaucoup et surtout qu'ils maîtrisent très bien. Ils se sentent vraiment à l'aise dans cette rhétorique qui par ailleurs est extrêmement problématique mais, en même temps, dans ces domaines du Cyber leur aisance remonte à très loin. Ma lecture est qu'on pousse plutôt vers un modèle plus stable, d'autant que les Russes et surtout les Américains sont confrontés à des conflits asymétriques qui les gênent et qui perturbent un peu le système, que ce soit l'Intelligence Community ou le reste.

Stéphane TAILLAT

Là, il s'agit plus de la dimension numérique. Je partage votre avis, cela peut évoluer dans l'autre sens et je le souhaite plutôt. Mais, le fait est qu'on a un candidat élu qui avait déclaré à l'avance que, de toutes les façons, les élections seraient truquées. Il se trouve qu'un certain nombre d'évènements rentrent dans cette espèce de narration, même si ce n'est pas vraiment le cas, ce qui induit, me semble-t-il, une sorte de méfiance. Donc, oui retrouver une opposition classique dans laquelle on est confortable, mais avec des éléments de méfiance qui font qu'il faut *de facto* réapprendre autre chose. Avec les Chinois, les Américains ont résolu le problème différemment, c'est-à-dire que, pendant cinq-six ans, les Américains n'ont pas cessé d'accuser les Chinois d'espionnage économique. Le chef de la NSA, Keith Alexander expliquait, il y a cinq ans, que c'était le vol le plus important de toute l'Histoire, que cela allait renverser l'équilibre entre les deux Etats, que c'était déloyal, etc., et finalement, par un jeu subtil, en septembre 2015, lors d'une visite à Washington, Xi Jinping a signé une espèce de déclaration mutuelle de non agression par rapport à la question du Cyber-espionnage, économique j'insiste.

Milad DOUEIHI

Mais, bien entendu, l'autre Etat se garde bien d'en faire mention. Il me semble que, dans toute votre présentation, on retrouve bien tout ce mouvement autour du statut de la force, de l'importance qu'elle représente surtout au niveau du numérique, de ce que cela modifie ou pas. Je me rappelle cette pensée très hégélienne selon laquelle *la force n'est puissante que lorsqu'elle ne s'exerce pas dans toute sa capacité*. Ce qui me semble plus intéressant encore est cet équilibre à trouver avec la soit disant « Cyber-guerre », peu importe comment on l'appelle, et je me réfère à cette très belle pensée de Pascal qui dit : *la force sans la justice est tyrannique et la justice sans la force est impuissante.* Dans le contexte actuel, comment parvenir aujourd'hui à un équilibre entre la justice (et quelle justice) et ces mécanismes ?

Et puis, un dernier point : j'avais suivi un peu les audits de Stuxnet, le nom donné au logiciel qui avait infiltré le système nucléaire iranien par la Toile : c'est tout de même grâce à un *backdoor* que le système a pu fonctionner. Sans le *backdoor*, il n'aurait jamais pu fonctionner en dépit de la qualité remarquable de son code de très haut niveau. Il fallait un *backdoor* pour donner les instructions, surtout qu'on a vu ensuite se déployer plusieurs variations de Stuxnet avec des effets intéressants mais juste comme tests. A mon avis, je crois que beaucoup de gens peuvent jouer avec ce code, mais jamais à ce niveau là.

Stéphane TAILLAT

Rapidement, pour réagir sur la force et la justice, sur le statut de la force, il est intéressant que vous citiez Hegel parce que je crois beaucoup que ce sont les deux manières d'envisager la force. La force est puissante quand elle ne s'emploie pas : ce n'est peut-être pas la situation « idéale », mais c'est possible parce qu'est associée à la force la notion de légitimité traduite par un consentement à son existence. Assez paradoxalement, mes travaux de recherches doctorales, il y a un certain temps maintenant, portaient plutôt sur les effets de la force, montrant que la force est capable de transformer, à une petite échelle, y compris des systèmes sociaux et politiques.

Sur le deuxième aspect, bien sûr Stuxnet est plus compliqué que ce que j'ai pu en dire. Je voulais souligner le fait qu'effectivement il y a un code de très haut niveau ; évidemment, sans la reconnaissance et sans le backdoor, il ne fonctionne pas. Mais, lâcher ensuite ce code dans la nature, puisqu'il s'y est retrouvé ensuite, est extrêmement dangereux. D'ailleurs, les Américains, pour d'autres technologies comme pour les drones d'ailleurs, croient beaucoup à l'idée que : *nous, nous le faisons, mais faisons attention, car nous risquons d'ouvrir un précédent, et nous craignons la réciprocité*. Et c'est toujours le cas ! J'ai beaucoup d'admiration pour eux, mais je sais aussi qu'ils sont parfois d'une naïveté confondante sur quelques sujets, ou en tout cas, ils ont une vision un peu différente de la nôtre. Ils craignent beaucoup la réciprocité et on aurait envie de leur dire : *vous n'aviez qu'à pas commencer* ! Mais dans le cas de Stuxnet, je rappelle aussi qu'ils avaient un objectif bien précis, freiner ce programme nucléaire et éviter que les Israéliens ne le freinent en bombardant, ce qui aurait entraîné davantage de problèmes.

Echanges avec la salle

Marc WATIN-AUGOUARD (Forum international de la Cyber-sécurité)

Je suis le co-fondateur du *Forum international de la Cyber-sécurité* qui réunit tous les ans six milles experts d'une soixantaine de pays sur les questions de Cyber-sécurité, Cyber-défense. Je remercie le professeur Stéphane Taillat pour son exposé et si vous me permettez, je voudrais faire quelques petits commentaires, sans faire un deuxième exposé. Quand on parle de Cyber-guerre, il y a bien sûr, Cyber dans la guerre et la guerre dans le Cyber et vous avez bien fait de rappeler qu'aujourd'hui le Cyber dans la guerre s'est complètement banalisé. Vous avez parlé de l'opération Orchard avec les Israéliens, mais depuis le Kosovo, il n'y a pas eu un conflit sans utilisation de l'arme numérique : en Syrie, en Irak, on le fait, l'armée française le fait.

Le problème de la guerre dans le Cyber nous ramène au droit des conflits armés, c'est le droit de Genève et des Protocoles de La Haye. Or, pour qu'il y ait une guerre, il faut qu'il y ait un ennemi. Vous l'avez dit vous-mêmes : *pas d'attribution, pas d'ennemi !* Regardez, par exemple TV 5 Le Monde : qu'a-t-on dit ? On a dit : *c'est Daesh !* Sauf que, lorsqu'on a remonté l'origine du code, on a découvert que c'était du cyrillique et que la Cyber-attaque était partie de Saint Petersburg et de Moscou. Alors, qui est-ce ? Daesh, qui a payé la mafia russe ? Le gouvernement russe, qui a payé la mafia parce qu'il n'était pas content de notre position en Ukraine et de la non vente des Mistrals, en faisant passer l'attaque pour une attaque de Daesh ? Donc au final, *ce n'est pas moi, c'est ma sœur qui a cassé le calculateur*, disait Evariste. On est vraiment là dans un problème d'attribution. L'Estonie en 2007 a été bloquée pendant plusieurs semaines, tout le monde avait dit : *ce sont les Russes, ce sont les Russes !,* mais on ne l'a jamais, jamais prouvé ! Et, si on avait voulu contre attaquer, 60 % des universités américaines auraient été détruites par la contre attaque, parce que l'Estonie avait été bombardée par les universités américaines, en attaque de rebond c'est-à-dire qu'en fait on était passé par ces universités américaines.

L'autre idée importante quand on ne sait pas quel est l'ennemi, c'est la question de la létalité de la force. Vous avez dit : *est-ce que la force est létale ? Est-ce qu'elle entraîne des morts ?* Mais, est-ce que la létalité vient forcément de la force ? Je vous donne un exemple : le 21 octobre dernier, aux Etats Unis, trente sites ont été bloqués : Twitter, eBay, PayPal, CNN, etc. Par qui ? Par un individu qui n'était pas content de sa Play Station et qui a loué dans le dark Net un réseau zombie d'ordinateurs, composé de cent cinquante mille caméras de vidéosurveillance qui avaient été piégées pour attaquer le serveur DNS Dyn. Cela veut dire qu'en fait un individu peut très bien aujourd'hui entrainer des conséquences importantes. Au cas présent, il n'y a pas eu de mort d'hommes, mais imaginez qu'on fasse la même chose sur les IRM, les scanners, les hôpitaux, le 15, le 18, le 112. Vous imaginez le nombre de personnes qui, même indirectement, pourraient mourir. Donc, tous les paradigmes sur lesquels repose la guerre aujourd'hui sont complètement remis en cause. Ce sont les mêmes armes parce que je peux utiliser le même Botnet pour empêcher Les 3 Suisses de fonctionner, pour accompagner une attaque terroriste classique, ou pour utiliser une attaque d'Etat. Donc, vous voyez que tout cela nous rend les choses très peu lisibles. Je ne vais pas poursuivre mais au sujet des Cyber-armes, dites vous bien qu'une Cyber-arme ne défile pas le 14 juillet ! Ce sont des armes one-shot, une fois que j'ai utilisé une Cyber-arme, elle est connue de l'adversaire qui trouvera donc la parade. Ce sont donc des armes un peu particulières.

Quand vous avez parlé des vulnérabilités, ce qui me paraît très important c'est qu'on raisonne avec les chiffres d'aujourd'hui : dix milliards de machines connectées aujourd'hui dans le monde. On sera vraisemblablement à mille milliards de machines connectées à la fin de la décennie prochaine, avec un Homme dans un ensemble systémique, entouré d'objets bavards, de relations « machine to machine » et non pas « homme-machine » et non pas « homme-homme » et nous serons, depuis la domotique, l'immotique, les espaces intelligents, les voitures intelligentes, etc., dans une espèce d'écosystème numérique qui sera extrêmement vulnérable à tous les effets « domino » : c'est peut-être votre réfrigérateur connecté qui rendra la ville entièrement inopérante. A mon avis, un des points les plus importants sera justement de voir comment éviter cette espèce de chaos Internet.

Enfin dernier point, et je terminerai là-dessus, vous avez raison d'insister sur les Cyber-attaques qui vont toucher les systèmes opérateurs d'importance vitale. Je suis près à parier avec vous (on se retrouve ici en 2030, mais je ne serai peut-être pas vivant) : que dira-t-on en 2030 ? On dira qu'on a réussi, grâce à toutes les actions menées en amont, grâce à l'intelligence artificielle, grâce aux Big Datas, grâce à ce qu'on appelle la *street intelligence*, à éviter par la défensive les Cyber-attaques sur les opérateurs d'importance vitale, sur les sous-traitants, etc. L'infrastructure sera donc protégée. Mais, qui va émerger, tout seul en rase campagne, victime de toutes les Cyber-attaques ? L'Homme ! La Cyber-attaque est constituée de trois couches : la couche matérielle (l'ordinateur), la couche logicielle (ce qui fait marcher l'ordinateur) et la couche cognitive, ce qui donne du sens. Or, nous sommes entrés dans la bataille du sens et la vraie guerre que nous allons mener, et que nous menons déjà aujourd'hui, est la bataille du sens pour savoir si, oui ou non, on sauve l'Homme dans cet espace numérique. Voyez comme on peut façonner l'opinion publique sur Twitter avec les robots en faisant croire que ce sont des milliers de tweets d'origine humaine ! Voyez comme aujourd'hui on peut utiliser Internet pour

faire passer des contenus. Je pense que demain la vraie problématique sera comment éviter l'attaque sur nos esprits et, si vous me permettez ici, aux Bernardins, sur les âmes.

Stéphane TAILLAT

Je suis tout à fait d'accord avec vous, général Marc Watin-Augouard, mais je vais laisser la parole à la salle avant de répondre.

Pierre GUEYDIER (Université Catholique de l'Ouest)

Nous sommes presque voisins puis que je m'occupe d'un Master *« Conflictualité et médiation »*. Je voudrais rebondir très brièvement sur ce qui a été dit et poser une question sur les capacités offensives en matière de contenus. J'avais eu l'occasion de discuter avec le général de corps d'armée Didier Castres, chef « opérations » à l'état-major des armées, et je lui avais posé la question de savoir qu'elles étaient, par rapport à la propagande de Daesh, à son sens, son contenu informationnel et cognitif, les capacités de réaction en termes de contre propagande. Il y a eu quelques tentatives récentes de Story Telling médiatique et numérique, mais cela fait maintenant quatre ou cinq ans que ces messages sont diffusés, mais là il y a mort d'hommes : des adolescents se font embarquer et éventuellement périssent, ou font périr d'autres par les attentats. Il y a vraiment une létalité assez réelle. Quelles sont les capacités d'offensive ? On touche, me semble-t-il, véritablement une question politique dès qu'on parle de contre propagande. On voit bien que, dès qu'on parle de contre propagande aux armées françaises, on touche évidemment un problème très compliqué. C'est donc bien le contenu sémantique qui transite par ces réseaux qui est, sans doute, le plus dangereux et le plus facile à manipuler à un moindre coût puisque l'asymétrie est considérable.

Stéphane TAILLAT

Je ne peux pas répondre de manière spécifique à votre question. Par contre, il y a une réflexion qui me semble évidente : les réseaux sociaux comme tout le reste (je n'ai pas suffisamment insisté sur l'aspect fragmenté du Cyberespace) servent de « chambre à écho ». J'aime bien l'expression, qui n'est d'ailleurs pas très utilisée en français mais plus en anglais : *echo chamber*. On le voit tous les jours sur Twitter et je l'ai observé notamment pendant les élections américaines : les gens ne se parlent plus que dans des cercles restreints et sans être spécifiques, on pourrait disposer de tous les moyens qui consisteraient à fermer tous les comptes, etc., mais cela serait extrêmement compliqué et demanderait la pleine et entière coopération de Twitter, qui ne serait pas d'ailleurs simplement une question de volonté mais aussi de capacité, en sachant en plus que les réseaux sociaux ont aussi une tendance naturelle à s'autoréguler, c'est-à-dire qu'on va signaler, etc. Donc, on peut avoir ces capacités là, mais la difficulté, me semble-t-il, vient du fait qu'on ne se parle plus selon les mêmes termes, selon les mêmes représentations du monde. Je ne dis rien de bien nouveau, mais il me semble que les réseaux sociaux ont tendance à augmenter cette fragmentation en « chambre d'échos ». Je vois bien ce que pourrait être une contre propagande au niveau de l'Etat, comme au niveau interministériel ou comme au niveau de la Défense ou d'autres, mais je suis toujours assez sceptique. D'ailleurs je me dis, et on le voit avec le discours qui passe actuellement à la radio, qu'elle est plus destinée à sensibiliser les familles, à rassurer les familles ou les gens touchés par le phénomène. Mais, à mon avis, elle ne dit rien et ne peut avoir aucun impact sur les gens qu'on veut cibler.

Henri PIGEAT (Editions de l'ILISSOS)

J'ai longtemps présidé l'Agence France Presse et j'ai animé ici même un séminaire sur le thème *« Médias et biens communs »*. J'ai été très intéressé par l'ensemble de votre exposé, mais en particulier par vos remarques sur les analogies vraies/fausses. Cela me rappelle une théorie, un peu oubliée maintenant, peut-être parce qu'elle a été dépassée et supplantée par la théorie de la dissuasion, celle qu'on appelait, il y a une quarantaine ou une cinquantaine d'années, la « guerre psychologique ». C'était très intéressant parce que c'était la recherche d'une déstabilisation de l'adversaire, à l'époque dans les territoires dits coloniaux, et c'est sans doute pour cela que la théorie a été démodée. Mais, la réalité reste très vivante et très affectée par les processus numériques que vous évoquez, c'est-à-dire l'utilisation, avec des moyens infiniment plus puissants que ceux existant dans le passé, des fragilités normales des sociétés ou de l'économie.

Or, nous sommes dans une période (depuis hélas bientôt huit ans) de déstabilisation économique profonde, pas encore surmontée, et dans une situation que je ne qualifierais pas de « déstabilisation » mais « d'évolution » du processus démocratique à cause justement du numérique. La démocratie ne fonctionne plus aujourd'hui comme elle fonctionnait il y a cinquante ans, pour de bonnes et de mauvaises raisons, et elle n'a pas retrouvé son équilibre. J'ajoute une remarque : on voit très bien en ce moment, toutes ces dernières semaines en particulier, que les réseaux sociaux sont en train de découvrir une notion qu'ils avaient tendance à mettre sur le côté, celle de la responsabilité. Toute information et toute distribution de messages engagent inévitablement une responsabilité. Les réseaux sociaux ont passé leur temps,

depuis leur création récente, à évacuer cela parce que c'est contraire à leurs intérêts économiques bien sûr, mais il n'est pas certain qu'ils puissent continuer ainsi. J'ai tendance à penser personnellement que l'âge d'or des Facebook et autres, j'entends l'âge d'or économique, est en train de se terminer. Je ne dis pas qu'ils vont aller à la ruine, ils vont réinventer certainement d'autres choses, mais le système va changer.

Donc, au-delà de cette remarque, j'aimerais vous demander, mais j'imagine que c'est le cas, quels types de comparaison avez-vous été amenés à faire, vous-mêmes et les équipes que vous côtoyez, notamment sur cette comparaison entre la situation présente et ce qu'on appelait autrefois la guerre psychologique et l'ensemble des phénomènes d'opinion, nationaux et internationaux, avec cette capacité nouvelle, assez facile maintenant, de pouvoir aller toucher l'opinion du voisin, qu'il soit un allié ou un adversaire ?

Stéphane TAILLAT

Merci de votre question qui est assez vaste et je vais donc répondre sur deux points. Tout d'abord, effectivement des recherches sont faites sur ce sujet là, peut-être pas précisément sur cette analogie là, en tout cas pas en France, mais aux Etats Unis, car les Américains ont moins de difficultés que nous à aller voir du côté de notre Histoire militaire, notamment celle de la guerre d'Algérie. J'ai surtout lu des choses sur les analogies faites plutôt avec des systèmes de propagande venant d'Etats totalitaires, mais l'analogie est imparfaite dans la mesure où la capacité à contrôler les messages est aujourd'hui de plus en plus centralisée. Je vais prendre un exemple : vous avez deux Etats aujourd'hui (ils ne sont pas que deux, mais ce sont les deux auxquels je pense parce qu'ils s'affirment là-dessus) dont la doctrine officielle est effectivement le contrôle de l'information à l'intérieur comme à l'extérieur. C'est d'abord la Chine bien entendu, qui fait carrément un filtrage et on sait aujourd'hui que ce filtrage est contourné, qu'il y a une espèce de dialectique sans cesse entre l'Etat qui veut utiliser Internet comme moyen de contrôle social et les individus qui veulent au contraire s'émanciper de ce contrôle social et politique. Et puis, le deuxième Etat est la Russie, qui est plus intéressant parce que la Russie a, elle, une vision offensive de la chose.

Je n'ai pas eu le temps de l'expliquer tout à l'heure, mais les Etats occidentaux ont pris la question du Cyber par le bas, à travers la question de son intégration dans les dispositifs déjà existants, notamment militaires, mais d'ailleurs c'est peut-être la raison pour laquelle on a du mal justement sur l'aspect que vous souligniez. Les Russes au contraire ont pris plutôt la question par le haut : d'un côté, ils ont une vraie volonté de promouvoir les messages de la Russie à l'extérieur, et on sait bien quels sont leurs moyens (vous parliez des bots sur Twitter, de « l'usine à trolls » du Kremlin, qui sont des choses aujourd'hui très connues), mais de l'autre, ils considèrent que c'est de la guerre, ce qu'on appelle un peu improprement la doctrine Valeri Guerassimov, du nom du chef d'Etat Major des armées russes actuel, qu'ils appellent eux la « guerre de l'information » en partant des prémices suivantes : *nous ne sommes ni en Paix, ni en Guerre avec l'Occident*. Donc, en fait, on ne peut pas l'affronter, mais il y a quand même quelque chose à faire.

Ma remarque est qu'en revanche des recherches ont été faites sur la réception des messages, tout comme des études ont été faites sur la guerre psychologique en Algérie et les raisons pour lesquelles cela ne pouvait pas marcher : oui, les messages sont capables d'avoir des effets, mais en fonction du contexte dans lequel ils sont reçus. Dans le domaine qui nous intéresse, il faut donc être capable d'une vraie technologie politique pour concevoir les messages qui résonneront le mieux avec les croyances, les mythes, les biais, les représentations de la cible. De ce côté-là, les Russes sont avec nous assez forts parce qu'il leur est très facile de jouer sur un certain nombre de mythes politiques qui restent prégnants en France, qui vont de l'extrême droite à l'extrême gauche, dans tout le spectre politique, par exemple le mythe de l'homme providentiel, et donc ils ont plus de chance que leurs messages soient entendus.

Vous avez raison de dire que les modèles économiques des réseaux sociaux sont peut-être en perte de vitesse, mais il me semble qu'ils existent, qu'ils sont aujourd'hui utilisés et que le caractère de fragmentation, de « chambre à échos » fait qu'on arrive à faire passer de temps en temps des messages et pour peu qu'on ait bien réfléchi à l'auditoire, ils seront reçus. C'est donc un très bon moyen. Ensuite, est-ce que ce moyen est capable de passer de l'effet de la réception à l'effet politique derrière ? Rien de moins sûr ! C'est tout le problème des armes psychologiques, dans lesquelles je rentre d'ailleurs la dissuasion et la coercition dont je parlais tout à l'heure. Je rappelle : la force ne sert pas avant tout à détruire et à tuer, elle sert à faire des dommages. Donc, son effet est peut-être cinétique et physique, mais il est aussi psychologique. Or, autant l'effet physique peut être contrôlé, autant il est plus difficile de contrôler l'effet psychologique. Exemple : un avion en Afghanistan passe au-dessus d'un village pour détruire un camion citerne, comme c'est arrivé à Kunduz dans le Nord de l'Afghanistan en 2009. Il s'agissait des Allemands qui se sont plantés sur ce coup là puisque le camion citerne a été détruit mais en même temps on a tué des gens. Par contre, l'effet recherché derrière comme par exemple, montrer qu'on est une force bienveillante, ou qu'on ne voulait cibler que ceux considérés comme étant les ennemis, est complètement raté puisqu'on a tué quantité de civils. C'est exactement la même chose pour les armes psychologiques : on est capable de toucher la cible, mais de là à ce que la cible fasse ce qu'on attend d'elle, c'est une autre affaire.

Donc à mon avis, cette question peut aller très loin : sur la question du bombardement stratégique par exemple, la croyance, très solidement établie dans l'entre deux Guerres, que *si on cible les civils, si on fait une bonne fois pour toutes du « carpet bombing » sur les civils, ils céderont et ils réclameront la Paix,* ne s'est jamais réalisée parce que l'effet psychologique de la force, que ce soit un message visant à sidérer, à séduire ou à choquer, ou que ce soit une bombe ou autres, est impossible à calculer et ce qui est encore plus difficile à calculer, c'est de s'en servir de levier pour atteindre quelque chose. Je ne sais pas si j'ai répondu à la question mais on élargit la question du numérique à quantité d'autres domaines.

Milad DOUEIHI

Ceci me rappelle le document publié par Donald Rumsfeld, Secrétaire à la Défense, pour faire modifier le « soft power » vers le numérique et la sociabilité, ce qui à mon avis était plus intéressant que de recourir à la guerre psychologique. Il y avait dans le concept quelque chose de plus complexe, de plus nuancé. Il avait consacré une vingtaine de pages à toute cette dimension pour l'associer au numérique. Mais, je reconnais qu'on est dans un autre registre.

Stéphane TAILLAT

On a parlé du côté « obscur » de la guerre psychologique, mais il peut y avoir effectivement cet autre aspect, celui de la diplomatie publique qui utilise le numérique. Ce n'est pas forcément évident parce que le message doit arriver à faire oublier le fait qu'on soit un représentant d'un Etat et que forcément, derrière, on ait des intérêts bien calculés, des arrières pensées. Evidemment, la question est alors celle de la légitimité, qui renvoie elle-même à toutes sortes de questions comme celles de l'autorité, de la légitimité, etc.

Milad DOUEIHI

Mais, il me paraît important malgré tout de tenir compte aussi de cet aspect là.

Pierre TARIF (Groupe ENGIE)

Bonsoir. Je suis directeur d'un système d'information dans le groupe ENGIE, je ne suis donc pas spécialiste de la Défense. Je me fais une réflexion sur le poids relatif du monde physique versus le monde numérique. Vous avez prononcé la phrase selon laquelle *le numérique était plus favorable à la défense*. Il me semble que le fait d'emporter la totalité des plans ou capter la totalité des informations de telle infrastructure ou de tel dispositif est carrément trivial aujourd'hui avec une clé USB, ce qui n'était pas possible auparavant. Vu comme cela, le numérique est au contraire de nature à réduire à néant toutes les défenses. C'est ma première réflexion et j'aimerais avoir votre retour là-dessus.

Autre remarque : le numérique offre des moyens nouveaux et on parle surtout de ce qu'on connaît. On a tous un PC, on a tous un téléphone, et chacun croit ainsi connaître le monde numérique, mais je serais très surpris que les systèmes d'armes sophistiqués ne développent pas des moyens numériques particuliers, notamment quand on voit les machines les plus puissantes qui existent aujourd'hui. D'ailleurs, ces machines les plus puissantes aujourd'hui sont des machines chinoises qui sont dans le Top 10 mondial. La machine la plus puissante est chinoise, pour faire des calculs de matrice, des calculs très puissants, et elle était même aussi puissantes que les neuf machines suivantes qui étaient, *grosso modo* toutes américaines. Donc, il est clair que les Chinois font des choses, mais on ne sait pas trop ce qu'ils font, et il me semble que les moyens numériques prennent une autre forme qui échappe au monde civil, de mon point de vue de civil, et j'aimerais savoir ce que vous en pensez ?

Stéphane TAILLAT

Sur votre première remarque, j'ai précisé que c'était *avantage à la défensive,* à condition de prendre en compte deux paramètres qui sont : d'une part, la sophistication « organisationnelle » de l'attaquant, c'est-à-dire *est-ce que cet attaquant sera capable en fait de mener une opération ?* car ce sont de vraies opérations ; et d'autre part, la nature de la cible, à la fois au sens de sa valeur aux yeux de la victime*, est-ce un enjeu extrêmement important* ? et en termes de capacités de défense, auxquelles je rajouterais d'ailleurs l'hétérogénéité des systèmes, parce que les configurations matérielles, logicielles, même dans des réseaux d'entreprises, sont hétérogènes. Oui, vous avez entièrement raison, certaines choses sont devenues plus triviales aujourd'hui. En revanche, je voulais porter l'attention sur les attaques qui auraient le plus d'effets en termes de létalité et de destruction.

Sur votre deuxième question, le cas Chinois est très bien étudié aujourd'hui. Deux remarques : la première, je pense à l'exemple de la société de sécurité Lockheed Martin qui est un bon exemple, puisque Lockheed Martin s'était fait voler en 2009 je ne sais plus combien de Gigas ou Téraoctets de données confidentielles, notamment les plans de l'avion de

chasse F-35, etc. Le problème est que voler des secrets est très bien, mais encore faut-il être capable de les intégrer pour en faire quelque chose, ce qui renvoie à ma notion de « sophistication organisationnelle ». Ma deuxième remarque renvoie à ce que vous avez dit très justement sur les capacités de l'ordinateur. En fait, les deux derniers présidents Chinois ont repris ce qu'avait lancé Deng Xiaoping à la fin des années 70, sur la modernisation en l'adaptant à la notion d'informatisation parce que pour la Chine il semblerait que la numérisation soit une condition *sine qua non* pour être une grande puissance. Evidemment, c'est peut être un bon outil pour aller se servir chez les autres et on comprend très bien que les Chinois soient allés chercher des secrets technologiques chez les autres pour gagner en avantages. Mais d'un autre côté, le vrai problème des Chinois est que la modernisation, la numérisation induit un certain nombre de vulnérabilités. Aujourd'hui, la focalisation exclusive de la Cyber sécurité en Chine sur la notion de « *information security* », leur fameuse Grande Muraille d'Internet, fait que les Chinois perdent chaque année des sommes considérables à cause de la Cybercriminalité. Les Indiens ont d'ailleurs un problème similaire, car ils ont tendance à se connecter n'importe comment sur le Wifi public qui est très bien développé, notamment, selon l'anecdote que j'avais lue, pour regarder entre autres de la pornographie en ligne qui visiblement est une consommation assez importante, ce qui donne typiquement une cible en or pour les cybercriminels, indiens en particulier. C'est comme en Chine où les Chinois sont les premiers acteurs de la cybercriminalité et les premières victimes aussi. L'autre problème est que la numérisation n'est une bonne chose qu'à la condition, encore une fois, de l'intégrer dans une structure. Si on parle de la numérisation militaire, il faut l'intégrer dans des structures de Force, ce qui est extrêmement compliqué.

Globalement dans mon exposé, ce que je voulais dire ce n'était pas tant que *ce n'est pas dangereux, ce n'est pas grave*, mais c'était de dire qu'il y a un pas entre ce qu'on est capable de faire et les effets que cela aura, notamment si on a des ambitions très élevées en termes de *je vais changer le monde, je vais devenir le plus fort, alors que je n'étais pas le plus fort*, et notamment toute la question de l'asymétrie dans le domaine numérique, c'est-à-dire tout le discours selon lequel *puisque n'importe qui peut, grâce à un ordinateur ou au téléphone portable, agir dans le Cyberespace, cela désavantagerait les plus forts qui eux sont très vulnérables et auraient plus à protéger,* est un discours qu'il faut relativiser, non pas parce que les actes malveillants n'y ont pas lieu (ils sont très nombreux, ils le sont de plus en plus et ils le seront de plus en plus) mais plutôt en termes de *que signifient ces actes malveillants ?* C'est-à-dire quels sont leurs impacts, leurs effets, leur capacité à produire des changements politiques, sociaux, etc. ?

Encore une fois, il n'y a pas de révolution 2.0. Ce n'est pas parce qu'on mobilise une centaine de milliers de personnes sur Twitter, encore faut-il faire en sorte que ces gens se retrouvent dans la rue et qu'ensuite ils s'organisent. Or, ce n'est pas sur Twitter qu'on organise les gens, bien au contraire la logique de Twitter est plutôt d'être très décentralisé. On l'a vu avec les émeutes de Londres à l'été 2011, une des émeutes les plus en réseau, avec des résultats, on l'a vu, simplement même en termes politiques, quasiment nuls, ce qui est l'opposé de l'asymétrie puisque l'asymétrie est la capacité à produire un effet extrêmement important avec peu de moyens. Là, on a l'impression qu'on déploie énormément de moyens mais que derrière, cela n'aboutit à rien. Pourquoi ? Parce que la puissance et la capacité de mobilisation est insuffisante. Il y a beaucoup de ressources numériques, encore faut-il être capable de les mobiliser et de les exploiter. C'est pourquoi je disais que les Etats restaient, à mon avis, principalement les plus à même de le faire.

Luc BARANGER (CHECY - Centre des Hautes Etudes du Cyberespace)

Je voulais revenir au cas américain et aux Etats Unis. Vous avez mentionné le « Cyber-Pearl Harbor », mais si on regarde un peu l'Histoire, on peut dire qu'il a eu lieu. Il a eu lieu le 31 décembre 1999 avec le Bug de l'An 2000 où, souvenons-nous, Bill Clinton nous avait annoncé pendant des mois, et encore juste avant, que ce serait la fin du Monde. Ma question est la suivante : n'est-on pas dans un effet de propagande, car je ne peux pas croire que Bill Clinton y croyait vraiment ? Cette histoire de « Cyber-Pearl Harbor » n'est-elle pas aussi un effet de propagande ?

Stéphane TAILLAT

Dans ce discours sur le « Cyber-Pearl Harbor », il faut distinguer deux choses : d'un côté, il y a effectivement le mythe « Pearl Harbor » qui va évidemment résonner chez tout le monde aux Etats Unis et d'un autre, cela renvoie au côté instrumental du discours, car ce n'est plus tellement de la propagande, mais plutôt l'idée de savoir quel est le but poursuivi quand on en parle de « Cyber-Pearl Harbor ». Certes, quand Leon Panetta, le secrétaire d'Etat, le dit en 2010-2011 c'est qu'il y pense comme une possibilité, c'est-à-dire qu'il attire l'attention sur le fait qu'il y a des vulnérabilités, qu'elles sont potentiellement critiques. Et c'est vrai, c'est ce que vous disiez, mon général : si on attaque le système de contrôle de l'espace aérien américain, il peut y avoir potentiellement des milliers de morts si on fait s'écraser tous les avions, etc. La question n'est pas : est-ce techniquement faisable ? La question est que c'est politiquement improbable, ce qui ne veut pas dire impossible, mais improbable. Dans le mythe de « Pearl Harbor », il y a en partie le fait qu'il y croit et en partie un discours de mobilisation typique des discours sur la sécurité.

Le principe du discours sur la sécurité est de désigner un objet référent (ce qu'il faut défendre), ensuite une menace (contre quoi) et enfin les aspects techniques (le comment). L'intérêt, cela a été bien démontré en Security studies, est

l'apparition d'un processus de dépolitisation : ce qui devrait être l'objet de débat (ce qu'il faut défendre et contre quoi) est très vite évacué du débat au motif que c'est un enjeu de sécurité national très élevé. Donc, paradoxalement, le « Cyber-Pearl Harbor » a eu, peut-être, un effet plutôt inverse, c'est-à-dire que c'est l'époque où Thomas Rid a commencé à écrire, c'est l'époque où il va commencer ensuite à être entendu, notamment à la NSA, etc., où il va parler de « Cyberwar hype », c'est-à-dire : *arrêtons d'en faire trop !*

Pour résumer ma réponse, il y a le mythe, donc un outil rhétorique très simple à utiliser, mais on pourrait en mobiliser d'autres, mais ce mythe s'inscrit dans un discours qui vise à faire de la Cyber sécurité un enjeu majeur, voir pour « Cyber Pearl Harbor » un enjeu existentiel puisque cela menace la survie des Etats Unis, leur indépendance politique, leur intégrité territoriale.

Frédéric LOUZEAU

Merci beaucoup. Deux précisions avant de nous quitter. Nous aurions souhaité avec Stéphane Taillat qu'un chercheur Américain puisse être associé à nos débats, mais les derniers évènements politiques nous ont rendu la tâche plus difficile. Nous ne désespérons pas d'en faire venir. Il y aura donc probablement une autre séance sur le sujet, dès que ce sera possible, si Tim Junio, chercheur à l'université de Sandford, vient en France. Nous avions aussi prévu d'inviter une chercheuse d'Harvard sur la Cyber-Paix. Donc, on vous recontactera lorsque nous aurons réussi à mobiliser ces chercheurs, car nous n'avons approché aujourd'hui qu'une partie du sujet.

Nos prochaines séances de séminaire doivent avoir lieu :

- pour le séminaire de cartographie le 22 mars 2017, sur le thème *« Handicap et numérique »*, avec deux chercheurs Audrey Bonjour, de l'université d'Aix-Marseille, et Jean-Paul Departe, du Centre mutualiste de rééducation et de réadaptation fonctionnelle de Kerpape, qui travaillent sur ces questions depuis très longtemps, ce sera une séance passionnante,
- et pour le séminaire de recherche avec Milad Doueihi le 3 janvier 2017.

Encore merci à notre intervenant. Bonsoir.

****