COLLÈGE DES
BERNARDINS

Chaire des Bernardins
2015-2017

L'Humain face au défi du Numérique

Séminaire du 7 décembre 2016
Intervenants : Stéphane TAILLAT

Synthèse : Maryvonne VALORSO-GRANDIN

Cyber Guerre - Cyber Paix
La conflictualité

Depuis quelques années, la Cyber-guerre est une question de plus en plus visible du grand public, d'autant plus sensible qu'elle impacte à la fois la confiance, que ce soit du côté de l'Etat, des individus ou du modèle économique et politique, et tout ce qui est de l'ordre de la trace, des données, de leur exploitation économique, mais aussi la conception qu'on peut avoir des notions de souveraineté, de territoire, de frontière, de gouvernance, questions qui rejoignent celles du statut du secret diplomatique ou de la cryptologie. Sans doute, est-ce pour cela que les sciences sociales se sont emparées de cette question, multipliant les approches du géographe, du sociologue, du politologue, de l'historien, de l'informaticien, etc. Pour en parler, Stéphane Taillat adopte le tropisme « relations internationales » et pose un préalable sur le terme de « Cyber-guerre » qu'il n'accepte que par convention car il lui préfère celui de « Cyber warfare » plus pertinent, le français n'ayant qu'un terme pour désigner une réalité complexe. Le mot « guerre » entendu comme l'équivalent du combat ne traduit que la pointe émergée de la guerre puisqu'en se limitant au warfare américain, elle ne restituerait pas la guerre dans la conduite même de la guerre : au-delà de la tactique et de la stratégie, l'affrontement et l'interaction des acteurs sont constitutifs de son sens. Thomas Rid n'a-t-il pas rappelé dans *« Cyber-war will not take place » (La Cyber Guerre n'aura pas lieu,* 2013) que la « Cyber-guerre » n'était qu'une métaphore car il n'y a guerre que sous trois conditions : la létalité (il y a guerre s'il y a destruction et éventuellement mort), l'instrumentalité (elle n'est qu'un moyen dont le combat est, selon Carl Von Clausewitz, la grammaire) et une logique politique (elle est soumise à des fins politiques).

Le combat numérique : létalité, instrumentalité et fins politiques

Quand on parle de Cyber-défense, évoque-t-on vraiment un combat, qu'il s'agisse d'une entreprise protégeant ses réseaux, ou d'un individu protégeant ses données pour évoluer en sécurité sur Internet, ou d'un Etat protégeant des infrastructures critiques, la stabilité de sa société ou la survie du régime ? Stéphane Taillat utilise l'expression de « combat numérique » car elle renvoie à l'idée que le numérique est un lieu où s'affrontent des forces et où peut se déployer de la violence qui, sans être létale, peut être psychologique ou physique, car *la force, la violence ne servent pas avant tout à détruire, à anéantir ou à tuer, mais ont principalement des effets psychologiques, notamment en matière d'anticipation de la souffrance ou des dommages,* comme le dit Thomas Schelling. Sur un plan instrumental, les outils numériques peuvent-ils être utilisés pour manœuvrer dans l'environnement numérique, par exemple les réseaux d'un adversaire, les siens propres voire d'autres réseaux ? Peuvent-ils l'être pour contrôler une action ou les effets d'une action ? Derrière ces questions pointe en filigrane celle de l'anonymat des attaquants, avec pour corollaire la notion d'attribution, c'est-à-dire la capacité d'imputer une action à un acteur.

Le numérique est-il un instrument fiable pour faire pression sur un autre ou le dissuader en lui montrant l'existence de moyens de contrainte ? Si c'est le cas, l'Histoire militaire et stratégique du 20e siècle a montré que les progrès technologiques n'étaient en général des armes « miracles » que pour l'attaquant, rarement pour le défenseur (Cf. Bernard Bodrie, *« Le nucléaire : l'arme absolue »*, 1946). Donc, selon Stéphane Taillat, le numérique n'est clairement pas un bon instrument puisqu'il se contrôle très mal ou ne peut l'être que sous certaines conditions. Pourtant, la plupart des Etats développent des politiques de Cyber-défense qui définissent le numérique non plus comme un enjeu de sécurité informatique, mais comme un enjeu de sécurité nationale voire internationale, donc un enjeu de niveau quasi existentiel (Cf. la gouvernance de l'Internet par les Etats Unis), s'abritant pour justifier leurs politiques derrière les risques de menaces ou de crises. Par exemple, citons l'attaque en 2007 par « déni de service » de l'Estonie attribuée à la Russie, ou l'utilisation en 2008 par la Russie de moyens numériques de propagande pour soutenir ses forces et affaiblir la Géorgie, ou l'attaque contre le système bancaire russe déjouée en 2016 par le FSB, rappelant les attaques passées des systèmes bancaires américains ou du groupe pétrolier Aramco en Arabie Saoudite. Donc, puisque crises et menaces il y a, les Etats auraient raison de définir le numérique comme un enjeu de sécurité nationale ou internationale.

Mais, on pourrait se demander, *a contrario*, si ce n'est pas justement parce que les Etats font du numérique un enjeu de sécurité nationale ou internationale qu'un certain nombre de crises sont devenues des crises ? L'hypothèse défendue par Stéphane Taillat se décline en trois points. D'abord, toute Cyber-attaque implique des mesures appropriées pour éviter les représailles, d'où une tendance à la retenue stratégique : l'attaquant cible des « cibles molles » qui ne peuvent pas se défendre ou représentent un enjeu faible pour la victime, en restant en dessous d'un certain seuil. Par analogie avec l'époque de la Guerre froide, s'instaure une situation de « stabilité/instabilité », où l'absence d'affrontement direct des protagonistes (stabilité) se solde souvent par leur implication dans des guerres périphériques (instabilité), dans un paysage sécuritaire marqué par une inflation d'incidents et d'attaques généralement plus sérieuses pour les entreprises et les individus que pour les Etats, vis-à-vis desquels elles restent en dessous du seuil où les dégâts induiraient une réponse de l'attaqué. Ensuite, il faut tenir compte d'une variable indépendante, la capacité de riposte de la victime, avec pour corollaire le risque d'aggravation des tensions ou des conflits voire, à propos d'une Cyber-attaque majeure, une guerre ouverte entre deux acteurs. La manière dont les attaques dans le numérique seront inscrites dans le droit des conflits armés dépendra pour une part de cette variable. Aujourd'hui, le *« Manuel de Tallinn »* (2013), rédigé par des experts de l'OTAN sous la direction de Michael Schmitt, a entériné l'application dans le Cyberespace du droit des conflits armés et du droit international, principes repris dans la doctrine de dissuasion américaine, mais également en Russie ou en France (Cf.*Livre Blanc sur la Défense et la Sécurité nationale,* 2013), l'idée étant qu'en cas d'attaque d'intérêts vitaux la réponse pourrait dépasser le simple domaine numérique. Enfin, une cause formelle d'ordre quasi structurel trouble le jeu, l'importance des représentations. Parler de Cyber-guerre, c'est toucher l'un des deux récits racontés depuis l'apparition du numérique avec d'un côté, un récit narratif qui insiste sur l'espace de liberté, d'émancipation, d'opportunité et de l'autre, l'idée que c'est aussi un espace de domination politique, militaire, ou inversement de vulnérabilité et d'attaque sur des réseaux critiques ou sensibles. Aujourd'hui, dans le Cyberespace, ce qui l'emporte n'est pas tant l'idée que chacun puisse gagner, coopérer dans l'environnement numérique, mais plutôt celle que c'est un espace de conflictualité, avec pour conséquence la méfiance.

Le numérique, enjeu de la conflictualité

La numérisation ne connaît pas de limites : l'ensemble des activités économiques, sociales, culturelles, politiques ou militaires sont fortement numérisées et l'accès à Internet est un phénomène mondial qui touche aussi bien les sociétés les plus développées que les pays émergents. Donc, à numérisation croissante, vulnérabilité croissante. Le code constitue une première forme de vulnérabilité, mais il y en a d'autres, comme les comportements des individus ou des organisations qui, sans être déterministes, sont conditionnés par des procédures, des habitudes, des biais et donc faciles à tromper. Selon Martin Libicky, *il n'y a pas d'entrée forcée dans le Cyberespace.* Le réseau adverse est un mur dans lequel il suffit de trouver les failles. Plus la numérisation s'accroît et plus s'accroît le sentiment de vulnérabilité, à la nuance près que la vulnérabilité n'est pas forcément équivalente à la menace car pour qu'il y ait menace, faut-il encore un acteur malveillant souhaitant exploiter cette vulnérabilité. L'autre enjeu au niveau international est le fait que le Cyberespace soit, bien que global et transnational, marqué comme tous les flux de la mondialisation par de fortes inégalités, disparités et par une structuration « centre-périphérie ». Tous les individus, toutes les organisations n'ont pas encore accès à Internet pour des raisons techniques, socio-économiques ou politiques, induisant ainsi une forme de marginalisation malgré une impression de répartition égale de la « couche cognitive » du Cyberespace. Dans le Cyberespace subsiste au niveau des ressources pour agir, contrôler ou détourner les flux d'informations, une très forte disparité entre les Etats et les autres acteurs, entre les Etats eux-mêmes, ce qui expliquerait, selon Stéphane Taillat, une lecture « hobbesienne » des relations internationales, où les Etats qui se sentiraient « exclus » ou « menacés » par la domination américaine pourraient réagir de manière à aggraver les tensions sur des domaines autres que l'économique, la souveraineté numérique ou la souveraineté, entravant ainsi toute capacité de coopération.

Alors, les potentialités de déclencher un conflit entre deux Etats sont-elles réelles ? Pour Stéphane Taillat, la réponse est dans ce qu'il appelle les deux faces des politiques de Cyber-défense. Les Etats étant seuls garants de leur sécurité, un Etat aura beau affirmer sa bonne foi sur ses intentions de coopérer, de faciliter la paix plutôt que la guerre, d'avoir un appareil de défense uniquement défensif, les Etats voisins, rivaux, voire ennemis ne prendront pas à la lettre ses dires, car pour être en sécurité un Etat est confronté à deux choix : soit il démantèle son dispositif de défense comme signe de bonne foi (cf. *non offensive defense),* le piège étant qu'en affirmant sa bonne foi il soit plus en insécurité, soit il augmente ce qui va garantir sa sécurité (alliances, système de défense, déstabilisation des potentiels adversaires) jusqu'à s'introduire dans les réseaux ennemis, rivaux voire alliés, au risque alors d'aggraver sa sécurité par effets d'action/réaction, les autres Etats pouvant prendre ses intentions comme suffisamment hostiles pour justifier des dispositifs de défense agressifs (cf. la course aux armements). Or, ce dilemme de sécurité des politiques de Cyber-défense élude souvent l'autre mode possible de défense, celui de la « guerre préventive » qui consiste à se prémunir en désarmant l'adversaire avant que la guerre ne commence. Le numérique a plutôt tendance à renforcer ce cycle de méfiance, alimenté à son tour par l'idée qu'on doit aller voir chez les autres ce qui se passe, si possible en évitant de se faire repérer pour ne pas alimenter les tensions. Or, souvenons-nous que, quand on parle d'attaque et de défense, d'offensive et de défensive, les rôles d'attaquant et de défenseur ne sont pas toujours aussi clairs. C'est là que le juriste, le politiste ou le stratégiste doivent rester attentifs, tout comme les décideurs politiques ou militaires, pour bien mesurer

que les rôles d'attaquant et de défenseur se définissent d'abord au niveau des objectifs. Par analogie à ce qu'on appelle les « deux âges nucléaires » (pendant et après la Guerre froide), le Cyberespace présente des cycles similaires d'instabilité, l'objectif d'atteindre le maximum de stabilité entre les Etats n'étant possible que si les Etats en question ont des objectifs politiques défensifs, comme par exemple un objectif de conservation du *statu quo* ou la volonté d'améliorer leur situation. Si les Etats ont des objectifs de remise en cause de l'intégralité de l'ordre international, en revanche la sécurité internationale pourrait alors se trouver compromise.

Le numérique, théâtre de conflictualité

Le numérique est donc un théâtre de conflit, avec néanmoins un décalage entre les pratiques et les représentations de la part de la pluralité d'acteurs qui utilisent le Cyberespace pour atteindre leurs objectifs politiques ou économiques. Mais quel est leur impact réel et celui des menaces qu'ils représentent ? Economiquement, la Cybercriminalité a le plus fort impact puisqu'elle pèse entre 400 millions et 4.000 milliards de dollars. Politiquement, l'écart est plus grand entre les impacts réels des menaces et la manière dont on en parle : beaucoup d'Etats, surtout l'Amérique, insistent sur le risque « Cyber Pearl-Harbor », c'est-à-dire celui d'une attaque catastrophique paralysant complètement l'infrastructure économique, politique voire militaire d'un pays et facilitant une attaque conventionnelle. Si l'idée que des acteurs ou des organisations pratiquant le terrorisme comme une stratégie puissent investir le numérique n'est pas à écarter, les menaces les plus fréquentes ne restent-elles pas le fait pour n'importe quel individu de se retrouver dans la situation où ses données ou sa carte bancaire soient vendues sur le dark Web, ou le fait que des Etats peu scrupuleux ou d'autres acteurs puissent utiliser des données plus personnelles ?

Dans le numérique, la réalité est tout autre du fait de ce qu'on appelle un effet de « longue traîne ». L'Internet, le Web 2.0 permettent à n'importe qui de s'exprimer, de mobiliser pour une cause, de diffuser de la propagande, y compris dans les endroits les plus reculés. Le Cyberespace facilite l'expression de projets politiques très marginaux en nombre de personnes touchées, mais qui arrivent à se parler et donc à exister. Mais quel est l'impact de ce qu'on appelle les « Révolutions 2.0 », l'idée selon laquelle grâce à Twitter, aux réseaux sociaux, des régimes politique pouvaient être renversés ? L'exemple des révolutions Arabes a montré que les « Révolutions 2.0 » n'existaient pas. Certes, elles peuvent mobiliser plus de monde, mais accroissent-elles la capacité d'implication individuelle des personnes dans une lutte ? Elles vont entendre les messages au plus grand nombre, mais accroissent-elles vraiment la capacité de ces messages à produire un effet sidérant sur toute une société ? Certes, des organisations seront capables d'augmenter une menace par rapport à la réalité de ce qu'elles peuvent vraiment faire, mais ne faut-il pas prendre la menace avec beaucoup de précaution dans la mesure où les réseaux sociaux ne permettent d'organiser qu'une opération égale à zéro ou presque ?

En faisant croire que beaucoup d'acteurs peuvent être en apparence dangereux, on assiste à un effet de résilience qui crée une illusion d'optique. Celle-ci rejoint ce que Stéphane Taillat appelle un « jeu de dupes » à plusieurs niveaux. Pour utiliser le numérique comme théâtre d'une opération de sabotage, de subversion, d'espionnage, il faut trouver les failles. La condition *sine qua non* pour que l'opération réussisse est la capacité à tromper les défenses de l'adversaire, cela étant plus vrai dans le numérique que dans d'autres théâtres d'opération ou d'autres milieux. La capacité à simuler, dissimuler, tromper le réseau, les systèmes, les utilisateurs adverses est un frein pour mener des opérations ambitieuses avec de vrais dégâts. Pourquoi ? Parce que cette capacité est variable, d'autant plus si le système visé est critique pour la cible, ou si l'attaque n'est pas très sophistiquée d'un point de vue organisationnel. Plus la cible représente un enjeu critique pour l'adversaire, moins l'attaquant est sophistiqué comme dans le cas des organisations non étatiques, et plus la capacité à duper sera faible. Pour exemple, le piratage en 2015 par le Cyber-Califat du compte Twitter du commandement de l'Armée américaine au Moyen Orient a eu un effet psychologique sans commune mesure avec la réalité de l'attaque d'un point de vue stratégique. Donc, plutôt que de voir le Cyberespace comme un espace homogène, il faut l'appréhender comme plusieurs sous-espaces où il y aurait un espace avec des « cibles molles » qui ne se défendent pas ou mal, ou qui ne sont pas du tout défendues ou ne représentent qu'un enjeu faible donc faciles à attaquer, et au-dessus, un Cyberespace avec tous les réseaux critiques, bien défendus et difficiles à attaquer compte-tenu de la très forte probabilité d'être repéré. Donc, pour maintenir un niveau de duperie/tromperie apte à garantir la sécurité opérationnelle d'une attaque, il faut rester sur de petites cibles, éventuellement s'attaquer à des systèmes marginaux, sans aller au cœur du réseau de l'adversaire.

Le numérique, outil de la conflictualité

Le degré de numérisation des sociétés ou des acteurs, leur degré de sophistication organisationnelle, est très inégal. Quand on s'intéresse à la Cyber-guerre ou la Cyber-sécurité, il est essentiel de replacer les opérations dans leur contexte : on ne peut pas comparer la Russie, la Chine ou les Etats Unis avec l'organisation Etat Islamique par exemple dont les acteurs n'ont le niveau ni de la NSA ni du renseignement militaire russe (GRU). Si on s'intéresse à *qui est capable ou qui est tenté d'utiliser le Cyberespace pour produire des effets ou atteindre des objectifs*, il faut plutôt regarder du côté des Etats, notamment les plus puissants, car en termes de légitimité politique ou de souveraineté d'un Etat les nuisances seront importantes. Aujourd'hui, les « capacités Cyber » sont intégrées dans les moyens traditionnels de la défense et de la guerre comme en témoignent un certain nombre d'exemples historiques sur la capacité d'utiliser les armes numériques comme des soutien ou des appuis à des opérations conventionnelles : citons les pratiques de

« défacement » de la Russie, l'opération américaine « Surch » de manipulation contre Al-Quaïda en Irak pour accélérer sa « destruction », l'opération israélienne « Orchard » contre le projet syrien de construction d'une centrale nucléaire à Deir ez au moyen de malwares pour tromper les radars de la défense aérienne syrienne, à l'image de Stuxnet trompant les systèmes de contrôle des centrifugeuses de Natanz. Donc, en cas de conflit ouvert, on peut imaginer sinon une Cyber-guerre du moins des forces qui utiliseront le numérique comme talon d'Achille pour frapper une cible ou comme « multiplicateur » de forces, mais toujours en appui et pas comme arme principale.

S'appuyant sur l'analyse de Thomas Rid qui place les « Cyber armes » sur un continuum (du pistolet de Paintball à la bombe à guidage laser), Stéphane Taillat explique que l'immense majorité des malwares se situe du premier côté du spectre, celui des armes très indiscriminées qui, bien que dangereuses à utiliser du fait de leur effet « boomerang », ne sont pas des agents intelligents. L'intérêt de ces outils réside dans la capacité à lancer une attaque de déni de service ou une attaque brute pour anéantir des sites Internet ou des réseaux, qui se révèlerait pratique pour appuyer, faire du *signaling,* montrer une menace. Or, des agents intelligents restent préférables pour réussir une manœuvre de duperie/tromperie des réseaux adversaires, Stuxnet étant certainement l'exemple ultime vu sa grande capacité d'adaptation pour discriminer, cibler et sa programmation lui permettant de ne se déclencher que sur des systèmes d'exploitation ou des configurations matérielles et logicielles bien spécifiques, faisant de lui un petit arsenal à utilisation unique, difficilement réutilisable sans réadaptation.

Partant de ce constat, comment replacer les armes numériques dans la stratégie internationale ? Des chercheurs et des praticiens arrivent à la conclusion qu'elles sont très utiles pour faire des opérations clandestines de type renseignements ou sabotage, subversion, espionnage, dans lesquelles, même si la victime connaît l'attaquant, celui-ci aura toujours la possibilité de dire *vous n'avez aucune preuve*. Pour autant, il est rare que ces opérations clandestines renversent le cours d'une guerre ou les rapports de force entre les Etats su la scène internationale, sauf malentendu car dans le domaine numérique, calculer exactement les conséquences des attaques reste compliqué, des effets imprévisibles n'étant pas à écarter malgré les contrôles. Donc, les armes numériques sont plus utiles pour les opérations clandestines qu'elles ne sont des outils de dissuasion ou de coercition. Aujourd'hui, si pour deux Etats se faire la guerre de manière frontale est très compliqué et même hautement improbable, par contre pour les Etats en rivalité, en compétitions musclées ou en désaccord très fort sur certains sujets, l'objectif reste : *comment faire en sorte que l'autre cède ?* La force militaire est bien sûr utilisée pour peser sur ce type de rapport, par la coercition (essayer de contraindre l'autre à céder) ou par la dissuasion (empêcher l'autre de manœuvrer pour me coincer), mais elle doit contribuer plus que jamais à la diplomatie (*la diplomatie sans armes c'est comme la musique sans les instruments*, disait Frédéric Legrand au 18^{e} siècle) dans une forme de complémentarité avec les autres outils de la politique étrangère. L'exemple de l'attaque sur l'Estonie confirme que le numérique n'est pas un instrument de coercition : l'aveu de la Russie d'être derrière l'attaque de déni de service induit des difficultés pour elle du fait du dispositif de l'Otan, mais le silence de la Russie laisse subsister un flou sur l'intention de l'attaquant et donc, pourquoi l'Estonie céderait-elle en laissant en place cette statue du soldat russe commémorant la fin de la Seconde Guerre mondiale, alors que, pour elle, elle commémore plutôt la présence soviétique.

En résumé, le numérique ajoute de la complexité mais ne révolutionne pas les relations politico-militaires. Comme on ne peut pas empêcher une attaque ou une agression numérique, les décisionnaires doivent être formés aux aspects techniques, opératifs voire politico-stratégiques du numérique. Il faut crédibiliser la dissuasion par des frappes limitées, en rappelant au potentiel agresseur le sérieux d'une menace de représailles, l'objectif étant surtout de limiter le nombre d'attaques. Contrairement à l'idée reçue que le numérique serait propice aux attaques catastrophiques contre lesquelles on ne pourrait pas se prémunir, aux motifs qu'en étant très numérisé on serait plus vulnérable, que les failles et les risques d'attaque seraient inévitables, le Cyber favoriserait plutôt la défense, en particulier des Etats soucieux de garantir la sécurité de leurs opérateurs d'importance, de leurs systèmes de défense militaire ou de fonctionnement de l'Etat, de la société et de l'économie. Au-delà de ces cercles, les attaques possibles seront d'autant plus à l'avantage de l'attaquant que les cibles seront mal défendues ou les enjeux mineurs. Pour Stéphane Taillat, le vrai problème n'est pas tant une guerre numérique qu'une guerre à propos du numérique, avec un fort risque d'escalade, d'où l'intérêt pour les Etats de pratiquer une retenue stratégique en ne frappant pas les systèmes jugés critiques ou importants par leur cible pour éviter tout risque d'être découverts et de représailles. S'agissant d'enjeux de sécurité nationale qui peuvent s'inscrire dans des tensions entre Etats, le risque est grand que des Etats considèrent qu'une attaque touchant leurs intérêts vitaux, matériels ou symboliques, puisse donner lieu à une réponse bien sûr juridique mais pourquoi pas militaire, le risque d'un mauvais calcul de la part d'un agresseur n'étant pas à exclure. Aujourd'hui, le risque le plus grave à propos d'une attaque numérique serait de se trouver face à un Etat révisionniste qui veuille réviser le système qui le mécontente en dehors des modes habituels de révision de l'ordre international, à savoir soit jouer les règles pour les redéfinir à son avantage afin de prendre une place plus importante dans le système, soit affronter en face à face le tenant du titre avec le risque que, celui-ci voyant venir l'attaque, frappe le premier. Le risque d'escalade peut donc provoquer un affrontement qui, sans être tout de suite un affrontement armé, pourrait accroître des tensions sur la scène internationale.

****