Cyberespace et géopolitique

Lorsque les cinéastes ou la DATAR s'essayaient à anticiper l'avenir dans les années 1980, robots ou voitures volantes revenaient en boucle, comme si **Fritz Lang** et son *Metropolis* avait imposé un modèle définitif. L'explosion d'internet fait partie de ces éléments décisifs dont l'écrasante prégnance est devenue incontestable à défaut d'avoir été anticipé, du moins dans les pays les plus développés. De quelques millions au début des années 1990, le nombre d'utilisateurs est en effet passé à plus de 3 milliards aujourd'hui. Ce nouvel espace que l'on associe aisément à l'intangible, mérite qu'on s'y attarde au-delà des évidences, souvent trompeuses. Du latin *spatium*, l'espace a d'abord renvoyé à une notion de temps, de moment, avant d'évoluer petit à petit vers une notion de lieu, voire de milieu. En philosophie, de **Kant** à **Bergson** pour ne citer qu'eux, le terme est caractérisé par ses extériorités, par ses étendues finies. C'est aussi le milieu idéalisé de nos perceptions, contenant tout ce qui est concevable.

L'espace peut avoir quelque chose de rassurant dans ce qu'il est défini, limité par nos perceptions. C'est de manière plus tangible l'un des objectifs réaffirmés du traité d'Amsterdam de 1997 que d'UE garantisse "*une espace de liberté, de sécurité et de justice*" ; ceci était déjà présent dès le Traité de Rome, dans son article 61 (1957).

Associée au préfixe cyber, la chose est nettement plus anxiogène. Ainsi en 2007, l'Occident découvrait, médusé, qu'un Etat, l'Estonie, pouvait être totalement paralysé par une attaque informatique de grande ampleur. Après 2010, la divulgation du programme *Olympic Games*, visant à attaquer le programme nucléaire iranien via le ver informatique *Stuxnet*, mettait sur le devant de la scène deux acteurs étatiques, USA et Israël. Ces deux puissances avaient usé du cyberespace comme d'un moyen de parvenir à des fins stratégiques majeures.

Comment le cyberespace impose-t-il une nécessaire réflexion autour des diverses échelles des enjeux géopolitiques ?

Avant tout chose, il sera nécessaire de prendre la mesure pleine et entière des concepts appelés à être développés. Ce faisant, il sera possible de mettre en relation les acteurs et forces dialectiques en jeux avant de passer en revue quelques études de cas afin de parfaire ce tableau initiatique.

I - Boite à outil : définition et concepts

A - Cyberespace, cet inconnu

==> Définitions

κυβερνητικός : doué pour le mouvement, action de diriger, de gouverner un navire.

Cybernétique : science des théories, des processus de commande, de communication, de régulation.

Le cyberespace est avant tout le lieu de la complexité. Il recouvre 3 choses :

* l'espace, c'est à dire un lieu fini, délimité.

* c'est le lieu de la "*dialectique des volontés contraires*" (**Beaufre**, 1963), donc de la stratégie.

* c'est aussi un ensemble d'acteurs, donc la nécessité de questionner la sociologie.

Pour les Etats, le cyberespace est une clé de leur pouvoir, mais aussi de leurs limites : renseignement, sécurité à toutes les échelles, action offensive sont autant de problématiques actuelles.

Le cyberespace est donc autre chose qu'Internet : c'est un outil technique, ce sont les Hommes et tout ce qui y circule.

==> Caractéristiques : 3 couches superposées

1 - une couche matérielle : ordinateurs, câbles, systèmes (pour faire simple le hardware)

=> il y a donc un enracinement géographique du cyberespace à travers les infrastructures de réseau, les appareils et leurs extrémités. Une des clés sécuritaires ici sera donc l'énergie : faire fonctionner, refroidir.

2 - une couche logique (pour faire simple le software, les logiciels)

=> codes de la machine = langage homme/machine, les programmes

*ces codes sont directement liés à l'Homme, aux techniciens. Il incombe donc aux Etats et aux entreprises concernés de former les ressources humaines nécessaires à la mise en oeuvre de cette couche décisive. De fait, le système éducatif et la capacité à former et s'adapter au rythme des évolutions technologiques deviennent totalement déterminants. Dans ce sens, les USA disposent d'un système éducatif très médiocre au niveau secondaire, compensé par la capacité à attirer les meilleurs cerveaux dans les universités. Mais cette capacité est par définition plus fragile que celle consistant à

compter sur un corps de techniciens formés à l'intérieur des Etats, même si plus facile à gérer sur du court terme. La formation tout au long de la vie nécessite infrastructures et personnels compétents qui sont autant d'investissement de long terme, parfois très couteux et peu efficients dans le temps politique, mécaniquement court. On citera la réforme du système scolaire finlandais entamé dans les années 1970 et qui n'a vraiment porté ses fruits qu'au début des années 2000 ...

*il faut aussi se garder d'occulter une variable essentielle : les erreurs de langage, de code informatique. Chacune constitue une faille or il y a toujours plus d'utilisateurs et de machines, plus de complexité, plus de risques d'erreur et ainsi moins de sécurité.

=> protocoles de réseau = langage machine/machine

*celui qui tient le protocole tient le réseau et donc la sécurité. Ceci doit être mise en perspective avec le monopole de la violence légitime de l'Etat tel que défini par **Weber**[1]. Ce monopole est remis en question dès lors que ce sont des entreprises ou des particuliers qui imposent leurs protocoles ...

3 - une couche sémantique, informationnelle = dimension sociale

=> données : source de richesse du **GAFA** (Google Amazon Facebook Apple) mais aussi, car ces entreprises sont concurrentes et qu'il faut se garder de tous raccourcis simplistes, **Baidu**, **Alibaba**, **LeEco** ou **Samsung** en Asie. Ces ressources sont définies par le Big Data dont voici la définition donnée par IBM : "*Chaque jour, nous générons 2,5 trillions d'octets de données. A tel point que 90% des données dans le monde ont été créées au cours des deux dernières années seulement. Ces données proviennent de partout : de capteurs utilisés pour collecter les informations climatiques, de messages sur les sites de médias sociaux, d'images numériques et de vidéos publiées en ligne, d'enregistrements transactionnels d'achats en ligne et de signaux GPS de téléphones mobiles, pour ne citer que quelques sources. Ces données sont appelées* ***Big Data ou volumes massifs de données".***[2]

=> information : ce qui est dit dans une communication

=> opinion collective : construite avec d'autres vecteurs traditionnels comme le cinéma, la presse etc.

Ici la notion de sécurité est intéressante à questionner : pour les Occidentaux, il faut maîtriser les couches 1 et 2. C'est exactement ce qui ressort de la stratégie définie par le département de la défense américain en 2011[3] qui accorde de manière explicite une importance plus grande à la couche matérielle. Or pour les Russes et les Asiatiques,

[1] *Le Savant et le politique*, 1917-1919, cycle de conférence à l'université de Munich
[2] https://www-01.ibm.com/software/fr/data/bigdata/
[3] *Department of Defense strategy for operating in cyberspace*, juillet 2011

la clé réside dans la couche 3. On retrouve cette approche dans la méthode de subversion (cf élection US et **Poutine** ...), classique depuis l'antiquité à relire **Sun Tzu**[4], **Polyen**[5] ou **Onasandre**[6] pour ne citer qu'eux.

A RETENIR

Le cyberespace, contrairement à une opinion courante et populaire, n'est pas Internet car ce dernier est mondial, mais pas universel contrairement au cyberespace. Poser la question de la sécurité c'est poser la question des connecteurs qui sont les points de fragilité. Question des infrastructures critiques : il ne pas sous-estimer la capacité de résilience car ceci reste des inventions humaines. Le danger est limpide : tout est cible du fait des interrelations croissantes.

B - La Géopolitique un concept porté aux nues puis méprisé qui redevient tendance

1945 : **Staline** interdit l'étude de la "science" géopolitique sur son territoire car elle est réputée allemande, donc fasciste.

2017 : tout est devenu géopolitique : les relations internationales, mais aussi le football[7], la cuisine[8] ou le cinéma[9].

==> Origine :

La géopolitique est née au tournant des XIXè et XXè siècle, à la confluence de trois phénomènes :

=> darwinisme social et rationalisme scientifique

=> développement d'une analyse géographique de plus en plus politique

=> volonté d'expansion des principales puissances industrielles et singulièrement de l'Allemagne, toute jeune née en 1870 de sa victoire sur la France impériale de Napoléon III.

Le mot apparait pour la première fois avec **Gottfried von Liebniz** en 1679 dans une tentative de classement des sciences. Il en fait "*l'étude de la Terre en relation avec le genre humain, impliquant l'étude de l'histoire universelle et de la géographie humaine*".

---

[4] *L'Art de la guerre* , VI siècle av. J.-C. – V siècle av. J.-C.
[5] *Stratagèmes*, IIè siècle
[6] *Stratêgikos*, Ier siècle
[7] https://www.monde-diplomatique.fr/mav/39/BONIFACE/55359
[8] http://www.iris-france.org/64697-geopolitique-de-la-gastronomie/
[9] https://www.cairn.info/revue-geoeconomie-2011-3-page-9.htm

==> Comment relier Géopolitique et sécurité ?

Les écoles anglo-saxonnes et allemandes réfléchissent entre la fin du XIXè et le début du XXè à construire la sécurité de leurs nations / peuples.

Exemples

Rudolf Kjellen[10], Suède fin XIXè : la sécurité d'un état ce sont les frontières naturelles, une puissance maritime, une unité de l'Etat, du Territoire et du Peuple.

Freidrich Ratzel[11], Allemagne, début XXè : la sécurité des USA est assurée par un vaste territoire entouré de deux océans. Pour lui il faut que l'Allemagne, pour sa sécurité, se dote d'un *Raum*, un sol nourriceur d'une population. On lui doit l'essai sur le *Lebensraum* qui sera lu par **Hitler** ...

Karl Haushofer[12], Allemagne, début XXè : utilise les travaux de **Kjellen**, **Ratzel** et **Mackinder**. Pour lui la sécurité économique c'est un *lebensraum* à conquérir. Il milite aussi pour la nécessité de réunir tous les peuples de culture allemande, le *Volksturm*. Attention, il est patriote pangermaniste (défendre l'Allemagne pas détruire les autres), pas réellement nazi.

Alfred Mahan[13], USA, XIXè : théoricien du Sea Power. Sécurité = une ile (Amérique) en quasi autarcie.

Halford J.Mackinder[14], Britannique, début XXè. Théorie des pivots stratégiques : "*Qui tient l'Europe orientale tient le Heartland(= coeur du monde). Qui tient le Heartland tient l'île mondiale (Eurasie). Qui tient l'île mondiale tient le monde*".

=> théorie de l'encerclement insulaire qui sera reprise pendant la Guerre Froide avec la question des alliances type OTAN, OTASE et Pacte de Bagdad dans les années 1950.

---

[10] *Stormakterna. Konturer kring samtidens storpolitik*, 1905 (trad. *Les grandes puissances*)

[11] *Die Vereinigten Staaten von Amerika*. 1878–1880. // *Anthropogeographie. Die geographische Verbreitung des Menschen*. 1882–1891. // *Völkerkunde*. 3 Bände, Bibliographisches Institut, Leipzig 1885–1901. // *Politische Geographie*, R. Oldenbourg, München und Leipzig 1897.

[12] *Geopolitik des Pazifischen Ozeans*, 1925 // *Bausteine zur Geopolitik*, 1928

[13] *The Influence of Sea Power upon History, 1660-1783*. Little, Brown & Co, New York 1890 // *The Influence of Sea Power upon the French Revolution and Empire, 1793–1812*. Little, Brown & Co, Boston 1892. // *The Interest of America in Sea Power, Present and Future*. Little, Brown & Co, Boston 1897

[14] "*The geographical pivot of history*". The Geographical Journal, 1904, 23, pp. 421–37. // "*Man-Power as a Measure of National and Imperial Strength*", National and English Review, XIV, 1905.

Des théoriciens français s'opposent à visions trop déterministes et promeuvent plutôt l'idée de la sécurité par la Nation qui n'est pas un territoire et un peuple avec des frontières naturelles, mais une mémoire et une volonté de vivre ensemble. Exemples de **Ernest Renan** (XIXè) et surtout **Jacques Ancel**[15] qui meurt comme résistant en 1943.

=> La géopolitique, délaissée après la chute du régime nazi, fait un retour en force depuis la fin de la Guerre Froide car les questions de sécurité entre Etats restent prégnantes.

SYNTHESE

Géopolitique n'est pas une science. C'est une méthode d'approche interdisciplinaire des Relations Internationales. C'est une étude des inerties physiques et humaines, des coopérations et oppositions entre unités politiques qui cherchent à assurer la sécurité et donc la pérennité d'une communauté dans l'histoire. La sécurité est un enjeu clé des relations internationales et dans ce sens la géopolitique une grille de lecture décisive de l'espace et donc du cyberespace.

C - Le champ de l'Imaginaire

==> Pourquoi traiter de l'Imaginaire ?

Ce champ, immense, est une porte d'entrée à des questionnements majeurs et fait partie de la couche informationnelle et donc sociale définie plus tôt. Par le biais de la Littérature, du Cinéma, de la Bande Dessinée, les auteurs explorent des pistes liées à leur époque et aux grands thèmes de la vie. Les travaux de **Joseph Nye**[16] ont en outre démontré l'importance décisive du *Soft Power*, défini comme la capacité à influencer les acteurs internationaux de manière douce, certes, mais néanmoins décisive. Ainsi la sécurité est une des questions clés traitées dans la science fiction ou les dystopies.

Ce sous-genre de la Science Fiction est apparu au milieu du XXème siècle avec les parutions de **Ievgueni Ivanovitch Zamiatine** , *La caverne*, 1920, *Nous autres*, 1920-1924, du *Meilleur des mondes* d'**Aldous Huxley** (1932), de *1984* de **George Orwell** (1949), ou encore *Ravage* de **René Barjavel** (1943).

[15] *Géopolitique*, Paris, Delagrave, 1936 // *Géographie des frontières*, Paris, Gallimard, 1938 // *Manuel Géographique de politique européenne. 2. L'Allemagne*, Paris, Delagrave, 1940

[16] *Bound to Lead: The Changing Nature of American Power*, New York, Basic Books, 1990.

Ce genre littéraire s'oppose à l'utopie : il met en avant une société imaginaire basée sur les craintes humaines. Les romans appartenant à ce genre sont souvent des anticipations mettant en exergue des événements apportant le malheur suite à un projet politique précis. Ils anticipent les dérives de la société et en exposent les conséquences : mondes apocalyptiques généralement dominés par des régimes totalitaires. L'ambition des auteurs est de nous mettre en garde contre l'égoïsme et l'inconscience des hommes : quelles conséquences pourraient avoir les catastrophes écologiques, la chute des démocraties, la corruption ? Jusqu'où faut-il aller au nom de la sécurité ?

==> Une influence sociale grandissante

Depuis le début des années 2000 ce genre semble avoir explosé. Les succès *d'Hunger Games* ou de *Divergente* en sont des exemples prégnants. Ils posent des questions décisives. Primo, loin d'être novatrices, ces oeuvres s'inscrivent dans une grille de lecture assez pessimiste de notre monde, porté sur les questions de sécurité. Ensuite ces approches, essentiellement occidentales, surtout étasuniennes, participent à une forme d'impérialisme culturel qui pose question et génère des tensions. Enfin, dans quelle mesure s'agit-il d'une grille de lecture du monde, de notre temps, ou plus simplement du seul Occident ? Pourquoi s'adressent-ils à la jeunesse, c'est à dire à ceux qui seront les futurs adultes et donc futurs électeurs ?

Ces questions illustrent la pertinence d'une analyse approfondie de la couche 3 définie par ailleurs, bien au-delà de la couche 1 privilégiée par le département de la défense américain depuis 2011.

II - Acteurs et forces dialectiques

A - Le questionnement d'échelle spatiale et temporelle

==> Etat vs Etat : la géopolitique et la paix au sortir de la Guerre Froide

L'une des problématiques posée par la chute du Bloc de l'Est en 1989 renvoie à l'apparent vide géopolitique créé. Lorsqu'en 1991 l'URSS disparait définitivement, les USA se retrouvent seule puissance dominante à tel point que **Hubert Védrine** a parlé d'Hyperpuissance[17]. L'un des axes de réflexion de la sécurité mondiale a alors gravité autour du rôle de Gendarme du monde défini par **G.Bush** au moment de la guerre du Golfe de 1990-1991, dans un cadre onusien et donc multilatéral.

[17] https://www.cairn.info/revue-cites-2004-4-p-139.htm

Discours du président des États-Unis George Bush au Congrès, le 11 septembre 1990

Nous sommes réunis ce soir, témoins dans le golfe Persique d'événements aussi significatifs qu'ils sont tragiques. […]En l'espace de trois jours, cent vingt mille soldats irakiens et huit cent cinquante chars avaient déferlé sur le Koweït, et marchaient vers le sud pour menacer l'Arabie Saoudite. C'est à ce moment-là que je décidai de contrecarrer l'agression. […]

Ce soir, je veux vous parler de ce qui est en jeu, de ce que nous devons faire ensemble pour défendre partout les valeurs du monde civilisé et pour maintenir la force économique de notre pays.

Nos objectifs dans le golfe Persique sont clairs, précis et bien connus. […] Ces objectifs ne sont pas seulement les nôtres. Ils ont été approuvés par le Conseil de sécurité de l'Organisation des Nations unies à cinq reprises ces cinq dernières semaines. La plupart des pays partagent notre volonté de faire respecter les principes. Et un grand nombre d'entre eux ont intérêt à ce que la stabilité règne dans le golfe Persique. Ce n'est pas, comme Saddam Hussein le prétend, les États-Unis contre l'Irak. C'est l'Irak contre le monde. […] Il est clair qu'aucun dictateur ne peut plus compter sur l'affrontement Est-Ouest pour bloquer l'action de l'ONU contre toute agression. Un nouveau partenariat des nations a vu le jour. […]

Aujourd'hui, ce nouveau monde cherche à naître. Un monde tout à fait différent de celui que nous avons connu. Un monde où la primauté du droit remplace la loi de la jungle. Un monde où les États reconnaissent la responsabilité commune de garantir la liberté et la justice. Un monde où les forts respectent les droits des plus faibles. […]

Il s'agit du premier assaut contre le nouveau monde que nous recherchons, le premier test de notre détermination. Si nous n'avions pas réagi de manière décisive à cette première provocation, si nous n'avions pas continué à faire preuve de fermeté, ce serait un signal donné aux tyrans actuels et potentiels du monde entier. […] Les récents événements ont certainement montré qu'il n'existe pas de substitut au leadership américain. Face à la tyrannie, que personne ne doute de la crédibilité et du sérieux des États-Unis. Que personne ne doute de notre détermination.

Bibliothèque présidentielle du Musée George Bush, College Station, Texas.

Divers penseurs s'emparent de la question et la géopolitique confirme son retour sur le devant de la scène :

*__Francis Fukuyama__, *The End of History and the Last Man*, 1992 : la fin de l'URSS marque le triomphe définitif de la démocratie et du libéralisme. C'est donc selon ces deux logiques que la sécurité entre les Etats va se structurer pour cet auteur. Il avait déjà exprimé cette thèse dans un article "*La Fin de l'Histoire*" en 1989 du ***National Interest***. Dans ce contexte l'explosion progressive d'internet devait, dans la droite ligne de l'euphorie liée à la chute du Rideau de Fer, permettre la diffusion de ces concepts occidentaux à travers le monde. La Chine intégrant l'OMC en 2001 suite à la volonté décisive de Bill Clinton, alors en fin de mandat, semblait aller dans ce sens. Le cyberespace engendrait une expansion des communications, libres de contraintes de temps et de distance dans le cadre d'un village mondial cher à Marshall McLughan, ce qui allait nécessairement propager les idées et les valeurs démocratiques et ferait même tomber les régimes autoritaires, fussent-ils les héritiers de Mao.

*__Samuel Huntington__ : dans divers articles et surtout dans son best-seller *The Clash of Civilizations* paru en 1993, pense que **Fukuyama** se trompe. La sécurité et la paix entre les Etats doit se penser non d'un point de vue idéologique mais d'un point de vue culturel. Il s'agit ici de questionner l'identité comme source de paix ou au

contraire de conflit. Les espaces culturels très différents poussent au conflit. Cette thèse a été remise au goût du jour avec les attentats du 11/09/2001 vue par les neo conservateurs US comme un affrontement civilisationnel entre Occident et monde musulman.

Donc, à travers ces exemples, la sécurité semble du ressort des Etats entre eux voire, à des échelles différentes, de blocs de civilisation définis par **Braudel** (*Grammaire des civilisation* - 1987) puis repris et ingérés par **Huntington**. Mais ceci devra être nuancé par une mise en perspective des inerties profondes.

==> Individu, Etat et espace cyber : sécurité et liberté dans les années 2000-2010

*Constat : l'espace cyber ne cesse de croître. En effet nous assistons au développement exponentiel des machines connectées, des adresses IP, des capacités de production et de traitement des données type *Big Data*. Le cyberespace s'immisce partout, le numérique connecte, mais aussi colonise via les robots, les smartphones et même les frigos. Villes, transports, énergie : autant de lieu et de secteurs qui sont englobés. ATTENTION : une part non négligeable de l'humanité reste en dehors de ce processus car le cyberespace est lié à la notion de développement donc ici les questionnements de sécurité ne sont pas - encore - universels. Toujours est-il que le bilan des attaques cyber de 2016 est sans appel. On citera celles, majeures, contre l'hébergeur français OVH ou la société américaine DYN[18] ; mais il ne faut pas oublier la multitude d'attaques de faible niveau contre des entreprises de type ETI ou l'usurpation d'identité ou l'attaque des hôpitaux britanniques de mai 2017.

*Le cyberespace est ainsi devenu un enjeu sécuritaire majeur pour les Etats : exemple des piratages des ordinateurs du Parti démocrate en 2016 dans la perspective des élections US attribués à la Russie. Mais aussi piratage en règle des réseaux ukrainiens lors de l'intervention russe en Crimée et en Ukraine entre 2014-2016 , Ukraine encore victime d'une attaque majeure dernièrement avec le malware *Crash Override*[19], attaque *Stuxnet* déjà citée par ailleurs. Dans le même temps, le monopole des Etats est aussi remis en cause ; ainsi le *Bitcoin*[20], cette monnaie virtuelle utilisée entre lors des attaques de type *Ransomware*, corrode frontalement le droit de frapper monnaie. Les Etats doivent contrôler le cyberespace (théorie de **Joseph S. Nye** sur le cyberpower en 2010), tout en posant la question de savoir si les petits Etats ont les mêmes objectifs ou dépendance que les grandes nations. Selon cette approche les USA sont clairement largement en avance. En 2010 a été créé le US Cyber Command, dirigé par le patron de la NSA. Les moyens humains et financiers sont sans commune mesure

[18] http://www.lemonde.fr/pixels/article/2016/10/21/une-cyber-attaque-massive-perturbe-de-nombreux-sites-internet-aux-etats-unis_5018361_4408996.html
[19] http://www.zdnet.fr/actualites/crash-override-le-nouveau-stuxnet-qui-s-est-attaque-aux-infrastructures-ukrainiennes-39853598.htm
[20] https://bitcoin.org/fr/

avec ce qui peut se faire ailleurs, du moins pour le moment. La NSA a mis en place un vaste système de surveillance reposant sur une collaboration étroite avec des alliés de premier plan, les "*Five eyes*" : USA, Canada, Royaume Unis, Australie et Nouvelle Zélande. Quatre autres nations peuvent compléter le dispositif, on parlera alors de "*Nine eyes*", avec la participation de la Norvège, du Danemark, des Pays-bas et de la France. Ces questions ne sont pas l'apanage de l'OTAN, la Russie ayant dès 2000 une stratégie de cybersécurité[21]. Mais ces systèmes et réflexions institutionnelles[22] ne doivent pas occulter une variable essentielle : Internet est pour le citoyen un espace de tous les possibles.

*Le citoyen est acteur essentiel de sa sécurité. Il donne de manière volontaire ou non des informations qui peuvent être utilisées pour ou contre lui par des entreprises telles **Amazon**, **Facebook**, **Alibaba** ou **Samsung**. Le citoyen peut également user du pouvoir du Cyberespace pour interagir avec les Etats :

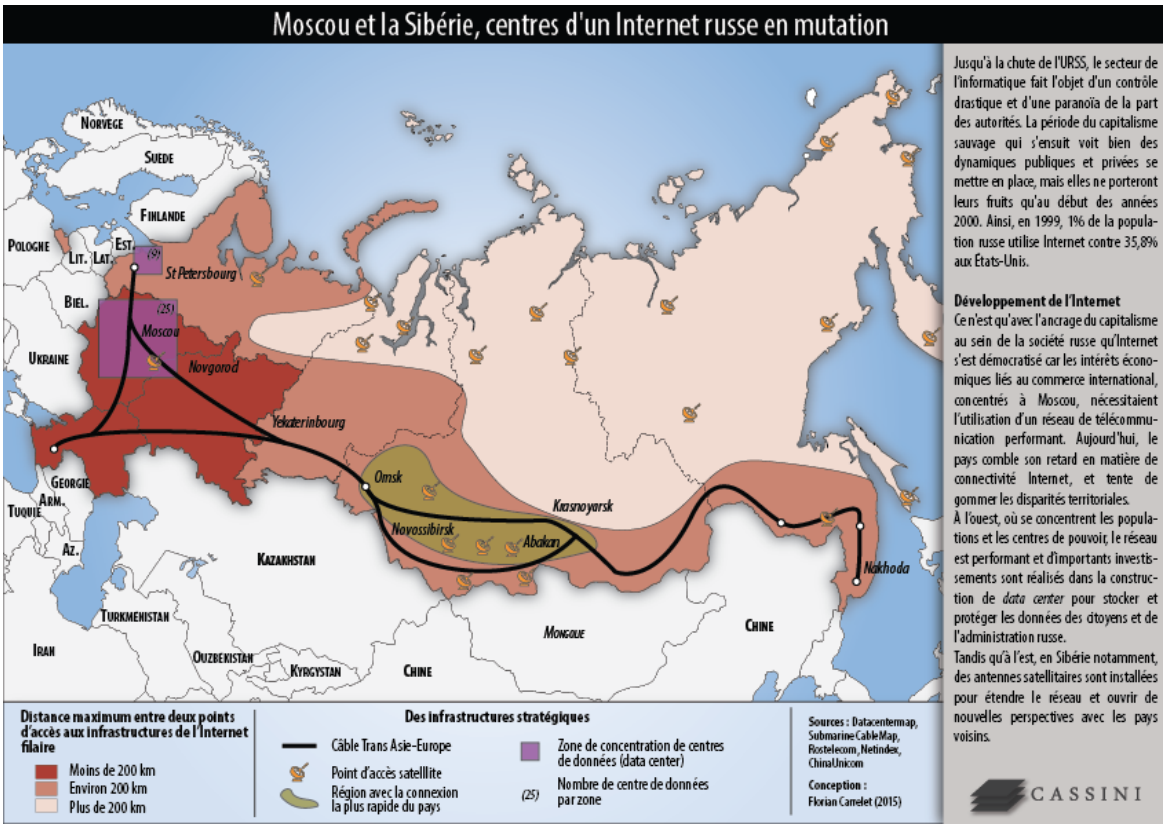
- Exemple des printemps arabes de 2010, poids des réseaux sociaux type Facebook : on a parlé alors "d'***empowerment***" du citoyen qui reprendrait la main sur les Etats, sur le politique. C'est aussi l'affaire **Snowden** (ancien de la CIA et de la NSA) de 2013 avec la divulgations d'informations sensibles et confirmant la mise sur écoute globale des citoyens via le *Système Echelon*[23]. C'est le citoyen, dans *Mr.Robot*, série télévisée américaine créée par **Sam Esmail** et diffusée depuis le 24 juin 2015 sur USA Network, qui est à l'origine d'une révolution totale du monde. La réalité n'est pas très loin de la fiction, que l'on songe aux ***Anonymous*** qui agissent depuis quelques années comme un groupe occulte de pression.

[21] The information security doctrine of the Russian Federation
[22] voir le rapport de l'OCDE de 2012 - *Cybersecurity policy making at a turning point. Analysing a new generation of national cybersecurity strategie for the Internet economy*
[23] https://www.monde-diplomatique.fr/mav/46/RIVIERE/1908

=> Le citoyen est donc une cible des failles sécuritaires : DAESH recrute en partie via le cyberspace, les multinationales pourraient prendre le pas sur les Etats et lui retirer, à terme, le monopole de la violence légitime (principe du *hackback* validé par les USA et le RU qui autorise une entreprise à riposter après une attaque cyber de ses réseaux : naissance d'un farwest numérique ?). Pour se prémunir de ce risque l'Etat doit contrôler le cyberespace et les citoyens. Mais alors quid de la liberté ? Une telle surveillance ne serait-elle pas le premier pas vers le totalitarisme ? Exemple du contrôle du net en Chine au nom de la sécurité du système.

*questionnement démocratique : aux USA comme en France, les dernières élections ont gravité pour partie autour de la sécurité, symbolisée par les frontières. Si, jamais, une frontière n'a arrêté durablement quiconque, si cet espace est d'abord dans l'histoire un lieu d'échange, il n'en reste pas moins que le citoyen voit dans l'Etat un organe capable de mettre en place des frontières efficaces pour sa sécurité. On retrouve ici le mythe du mur, mythe d'ailleurs réactivé autour du cyberespace et des firewalls[24]. La différence fondamentale est que les Etats gèrent la couche 1, c'est à dire les infrastructures. Ainsi, par exemple, le point d'entrée du Net en Russie se fait par les bureaux de l'ancien KGB à Saint Petersbourg depuis 1991 selon une architecture directement héritée de la Guerre Froide. Dans cette logique, les deux principaux hubs sont des villes dédiées à la recherche militaire, Ekaterinbourg et Novossibirsk[25].

[24] Un *firewall* est essentiellement un dispositif de protection qui constitue un filtre entre un réseau local et un autre réseau.
[25] Voir https://www.diploweb.com/Vers-un-Internet-russe.html



Quant à la Corée du Nord, la Chine ou l'Iran gérant totalement l'accès au net (voir les accords entre Google et Pékin), ils sortent de la sphère occidentale. Mais la Turquie, membre éminent de l'OTAN, procède des mêmes méthodes depuis le verrouillage du pouvoir par M. Erdogan. Dans ce cas de figure la frontière étatique fonctionne ... mais quid de la démocratie ?

B - Focus temporel : les inerties post Guerre Froide et le temps long

==> sécurité ou intérêts stratégiques ?

Partant de l'idée de **G.Bush** que le Nouvel Ordre Mondial hérité de la fin de la Guerre Froide obligerait les USA à assurer un rôle de garant sécuritaire du monde, dans le cadre multilatérale de l'ONU, il est possible d'interroger les faits.

=> **Zbigniew Brzeziński**, professeur et diplomate américain, ancien conseiller de **Jimmy Carter** (entre 1977-1981) apporte une réponse claire en 1997 dans *Le grand échiquier : l'Amérique et le reste du monde*. Pour lui ce n'est pas un quelconque devoir sécuritaire qui doit structurer la position des USA dans les relations internationales mais une réflexion autour des éléments qui permettent d'assurer la domination du monde par les USA. Dans ce sens seule la sécurité des USA compte. Le cynisme est assumé : "*puisque la puissance sans précédent des USA est vouée à décliner au fil des ans, la priorité géostratégique est donc de gérer l'émergence de nouvelles puissances mondiales de façon à ce qu'elles ne mettent pas en péril la suprématie américaine*".

La question de la sécurité est donc secondaire ici, celle des intérêts des USA prime. Cette logique doit être mise en perspective avec les choix des différents présidents depuis **G.Bush** jusqu'à **Trump**. Pour le moment il y a une remarquable continuité y compris lors de la présidence **Obama** qui a toujours mis en avant les intérêts US (voir l'étude approfondie de **Olivier Zajec**, La nouvelle impuissance américaine, 2011).

==> La Guerre Froide : un conflit qui écrase dans la seconde moitié du XXè siècle les logiques de réflexion géopolitique sur la sécurité du monde ?

Il est aisé de prouver le contraire :

*rupture entre Chine et URSS en 1959 : deux états communistes certes, mais surtout deux états en concurrence depuis des siècles pour étendre leur influence en Asie.

*1969 : Ostpolitik de **Willy Brandt** entre RFA et RDA car la Mitteleuropa est une sphère d'influence majeure de l'Allemagne en Europe, concurrencée ici par l'URSS.

*1978 : guerre entre le Vietnam et le Cambodge, deux états communistes qui, au-delà de l'idéologie, sont d'abord en lutte pour le contrôle du delta du Mékong.

*1980-1988 : guerre Iran-Irak, Arabes vs Perses, Sunnites vs Chiites, loin des logiques purement liées à la Guerre Froide.

Et après la Guerre Froide :

*Conflit en Ex-Yougoslavie, partition de la Tchécoslovaquie, conflit actuel en Syrie et en Irak : autant d'exemples de prégnance du temps long.

Donc à retenir : si la sécurité du cyberespace est devenue un enjeu majeur des relations internationales, il faut l'aborder avec les bons outils et les nécessaires changements d'échelle spatiale et temporelle, deux adjectifs aux sources du mot espace. Les acteurs sont complexes, les mutations en cours profondes, mais pas plus que les inerties.

III - Mise en application de ces principes

A - Les évolutions en cours

En liminaire il apparaît opportun de préciser les évolutions en cours, telles que définies par **Daniel VENTRE**, titulaire de la chaire de cyberdéfense et de cybersécurité de Saint-Cyr dans un article du hors-série 52 de DSI.

=> la guerre de l'information bat son plein. Plus que d'une reprise, on parlera de continuité, car l'effondrement du Bloc de l'Est n'a pas mis fin à l'Histoire. Les hackers

des années 1990 n'ont pas disparu, mais ont évolué en groupes de plus en plus structurés (*Anonymous*). Quant aux Etats, force est de constater que la dernière élection présidentielle aux USA a montré à l'envie la guerre d'information autour des cas **D.Trump** et **H.Clinton**, la Russie semblant être clairement identifiée comme un facteur de déstabilisation des opinions publiques via le Net.

=> de la difficulté de maîtriser les faits. Nombre d'attaques ne sont pas détectées et restent hors du champ d'étude ; ceci n'empêche pas qu'elles existent. Le processus des "*fake news*" joue aussi à plein, intoxiquant les services et rendant plus difficile une lecture pertinente de certains faits. Quant à la multiplicité des récits, repris, amendés par les réseaux sociaux, ils entraînent une saturation de l'information. Ici c'est la masse qui s'avère contre productive. Les derniers attentats en France ou au Royaume-Uni laissent à penser que les informations existaient, transitaient par les services sans qu'on puisse réellement les exploiter du fait de leur masse critique et du manque de personnel.

=> enfin, le cyberespace est devenu un domaine à part entière de l'action stratégique. C'est un moyen d'action (virus *stuxnet* contre l'Iran permettant d'entraver la course vers une éventuelle arme nucléaire, action russe en Géorgie en 2008 ou en Ukraine en 2014) et potentiellement une cause de conflit. Selon l'article 51 de la Charte des nations unies, une attaque cyber pourrait constituer une agression armée et donc donner droit à l'invocation de la légitime défense. Le Manuel de Talin 2.0 (The International Law Applicable to Cyber Operations - *Cambridge University Press* mars 2017) va clairement dans ce sens.

Prolongeant cette réflexion, les chercheurs du CLTC (*Center for Long-Term Cybersecurity*) de l'université de Bekerley ont proposé 5 scenarii pour 2020 :

1 - *The New Norman* : insécurité généralisée des réseaux. Seuls ceux qui ont la capacité financière peuvent se défendre. Résilience impossible pour les moins fortunés qui doivent se déconnecter.

2 - *Omega* : un algorithme permettant le profilage des citoyens-consommateurs pour anticiper leurs comportements. Ici *1984* de **Orwell** n'est plus très loin.

3 - *Bubble 2.0* : effondrement du **GAFA** et remplacement par la sphère d'influence asiatique. L'UE est épargnée du fait de sa législation sur les données personnelles.

4 - *Intentional Internet of Things* : les objets connectés envahissent la vie quotidienne et facilitent de fait la surveillance généralisée ce qui va dans le sens des gouvernements autoritaires. L'UE résiste pour les même raisons que celle du point précédent.

5 - *Sensorium* : les foules sont manipulées grâce au suivi collectif des capteurs connectés et du traitement du *big data*.

Il ressort donc des évolutions récentes que les Etats, quelques soient leurs niveaux de puissance, se testent. Les attaquent sont nombreuses, 304 millions d'attaques en 2015, et il n'y a pas de domination du cyberespace par une puissance unique. Les USA, censés être en meilleure posture du fait du **GAFA** mais aussi de **Tesla** ou **Uber** et de leurs investissements majeurs dans le domaine, sont sous la menace de la Russie ou de la Chine. L'Occident, riche, puissant, normatif dans le domaine du Net, semble avoir été attaqué par une puissance militaire relative, la Corée du Nord, technologiquement dépassée quant à ses matériels conventionnels et ses vecteurs, au printemps dernier[26]. De l'aveu même de hackers professionnels, la gène engendrée par cette nouvelle affaire de *ransomware* était sans commune mesure avec la simplicité du code[27]. Si la question d'un Cyber Pearl Harbour est parfois posée et contestée (Pearl Harbour n'a pas été déterminant pour le Japon sauf à précipiter sa chute, le relatif succès tactique se transformant très vite en catastrophe stratégique), le fait est que les certaines puissances se dotent, ou cherchent à le faire, d'armes à impulsion magnétiques telles le missile *Champ* de Boeing.

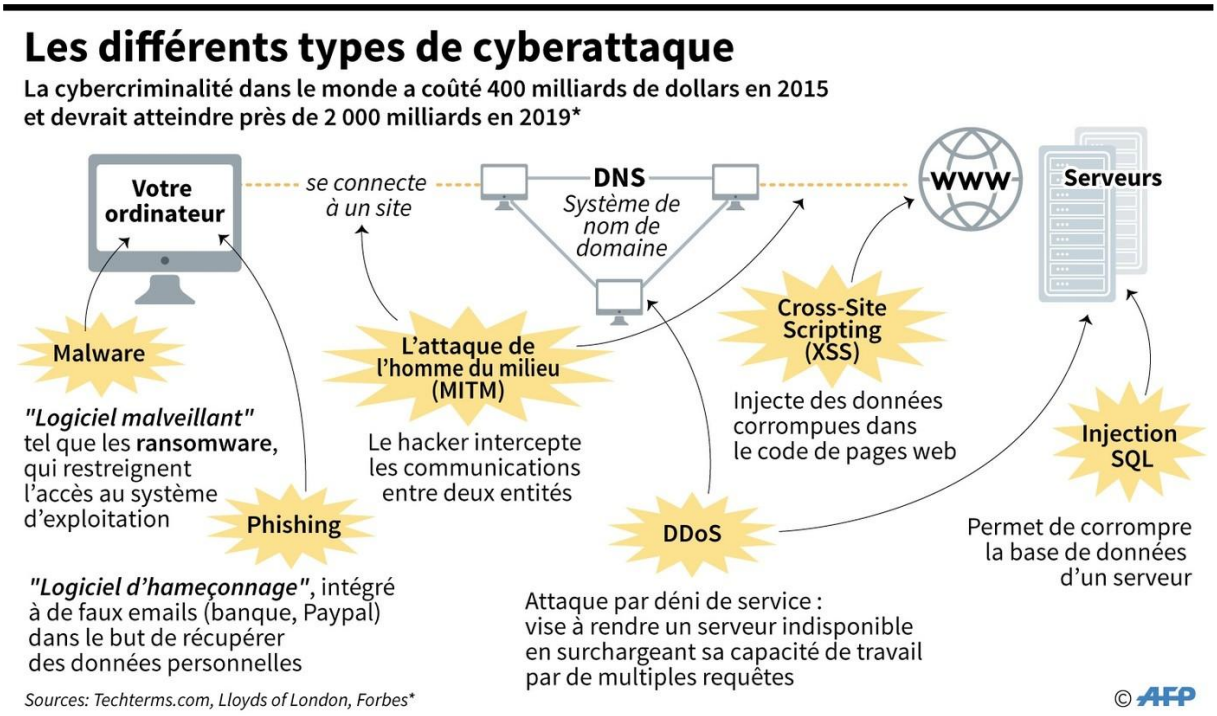
Le 12 décembre 2016 **Jean-Yves Le Drian**, alors ministre de la Défense, définissait dans un discours au centre DGA Maîtrise de l'information de Bruz, les contours du Commandement des Opérations Cyber entré en service le 1er janvier 2017[28]. Il ressortait de cette initiative majeure la volonté de sécuriser les réseaux, de construire un véritable pôle défensif, un pôle d'action numérique et une mise en place d'une réserve cyber de qualité. La France semble avoir pleinement pris la mesure des défis majeurs à venir, reste à passer aux actes avec les moyens nécessaires.

---

[26] http://www.lepoint.fr/high-tech-internet/la-coree-du-nord-pourrait-etre-derriere-la-cyberattaque-mondiale-16-05-2017-2127639_47.php

[27] http://www.zdnet.fr/blogs/green-si/heureux-comme-un-wanacrypt-dans-un-jeu-d-applications-obsoletes-39852428.htm

[28] http://www.opex360.com/2016/12/12/la-france-va-se-doter-dun-commandement-des-operations-cyber/



B - Le milieu maritime comme espace clé

L'espace maritime semble restreint aux seules problématiques de la Marine. Cet angle de vue est trop réducteur, qu'il soit permis de rappeler quelques chiffres et faits clés.

A l'échelle mondiale le monde maritime pèse pour plus de 1500 milliards d'euros. 90% du fret international et 50% des communications transitent par les océans, lesquels renferment 84% des minerais et des matières premières nécessaires au fonctionnement des économies développées. Enfin, 80% de la population mondiale vit sur une frange littorale de moins de 200km de profondeur (voir **Frémont A.**, *Les routes maritimes : nouvel enjeu des relations internationales*, Revue internationale et stratégique n69, ou **Desclèves E.**, *La mer, vecteur et enjeu du futur*, Etudes, n.418).

Les économies terrestres sont donc totalement liées à l'espace maritime et la projection de forces terrestres nécessite la maîtrise des mers, ne serait-ce qu'à échelle régionale. La puissance aérienne peut, sur le court terme, déployer des forces mais sans approche maritime minimale des opérations, ces dernières semblant possibles uniquement par voie aérienne pour les seuls USA. C'est l'un des enjeux clé de la base de Tartous en Syrie pour la Russie[29] ou du Collier de perle de la Chine[30].

Ceci étant posé, la sécurité cyber de l'espace maritime est confronté à des problématiques complexes. Tout d'abord, les points de connexion sont légions : des

[29] https://sptnkne.ws/dsSH
[30] https://www.cairn.info/revue-outre-terre1-2010-2-page-187.htm

ports, qu'il s'agit de protéger par voie terrestre pour le coup, aux navires et infrastructures de plus en plus connectés comme le montre la réflexion suivante[31].

L'École Navale, Télécom Bretagne, DCNS et Thales se sont associés pour créer en octobre dernier avec le soutien de la région Bretagne une chaire de cyberdéfense des systèmes navals à laquelle le Pôle Mer Bretagne Atlantique est partie prenante au sein du Comité de pilotage.

La mise en réseaux des systèmes d'informations expose à de nouveaux types d'attaque, les cyberattaques, dont il est nécessaire de se prémunir, d'où l'origine du concept « Cyber Défense ».

Couvrant les volets enseignement et recherche, cette chaire industrielle ambitionne de stimuler la cyber-innovation en se concentrant en particulier sur les systèmes navals et le domaine maritime. Elle aura notamment pour vocation de répondre aux problématiques de vulnérabilité des navires à la mer (navires de guerre, méthaniers, porte-containers...) dotés d'installations informatiques et électroniques complexes et d'équipages réduits (et notamment en l'absence d'expert en cybersécurité à bord), susceptibles d'être exposés à des cyberattaques aux conséquences potentiellement gravissimes.
C'est déjà le cas du projet DEAIS, labellisé par le Pôle Mer Bretagne Atlantique en 2014, porté par l'Irenav, Aremines, le Cerema et l'Université de La Rochelle, visant à identifier parmi les messages AIS, ceux qui pourraient avoir fait l'objet d'une falsification.

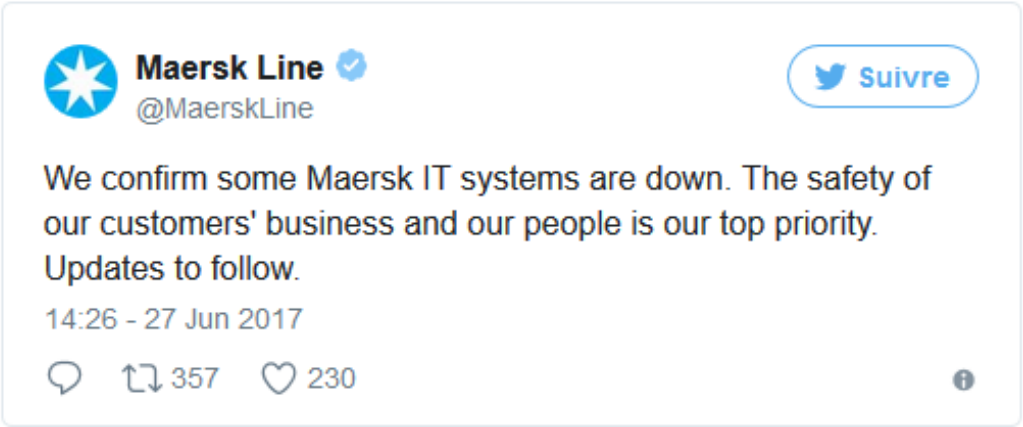
La chaire de cyberdéfense des systèmes navals animée par le Dr. P. Hebrard est placée sous le haut parrainage de l'Officier général Cyber de l'état-major des armées. Les travaux de la chaire se feront également en étroite coordination avec la Direction générale de l'armement (DGA).
La création de cette chaire s'inscrit dans la continuité du pacte Défense Cyber, présenté par le Ministre de la Défense en février 2014 et représente également une nouvelle concrétisation de ce Pôle d'Excellence Cyber (PEC), implanté en Bretagne avec une portée nationale et un objectif de rayonnement international.

L'attaque cyber d'un port n'est pas de l'ordre du fantasme. La superficie des ports de Marseille-Fos (12000 hectares soit la superficie de Paris) ou de Toulon (20 000 personnes y travaillent, civils et militaires), impliquent des moyens de surveillance énormes. Une simple clé USB peut servir à poser des malwares, moyen d'autant plus simple que ces infrastructures mêlent unités militaires comme civiles. Le piratage des espaces de contrôle, caméra par exemple, pose problème car ces dernières pallient les moyens humains et les sous-effectif. Faut-il rappeler qu'en 2011 le second port

[31] http://www.pole-mer-bretagne-atlantique.com/fr/actualites/12-la-vie-du-pole/1641-la-cyber-defense-un-enjeu-majeur-pour-le-maritime

européen, Anvers, a vu une mafia pirater le système de surveillance, afin de faciliter un trafic de stupéfiant en provenance d'Amérique du Sud[32]. Les logiciels utilisés dans ces lieux sont généralement issus du civil : système d'exploitation de *Linux*, *Microsoft*, voir dans certains cas *Android*. Aucun n'est à ce jour exempt de faille. Pire, ces programmes dépendent de puissances tierces qui, alliées, peuvent aussi disposer de porte d'entrées dans nos propres infrastructures[33].

Quant aux navires ou aux entreprises de transport, la dernière attaque cyber en date laisse songeur : fin juin 2017[34] *Maersk* s'est retrouvé incapable de planifier le transport de conteneur pour quelques jours avec à la clé des pertes financières non négligeables. Le pilotage automatique de ces monstres des mers induit la possibilité qu'un piratage pourrait entrainer l'échouage d'un navire, avec à la clé catastrophe écologique (marée noir en Méditerranée par exemple), économique pour l'entreprise ou la région concernée et, surtout, humain (un paquebot de croisière transporte près de 5400 personnes pour les plus gros).



Cible majeure aux répercussions gravissimes dépassant le seul cadre maritime, les mers et océans offrent aussi une base de réflexion quant à la stratégie appliquée au cyberespace. Suivant les réflexions de **Gille Deleuze** ou de **Laurent Henninger**, **Joseph Henrotin**, chargé de recherche au CAPRI, rappelle avec raison (DSI 52 - cf infra) "*qu'une véritable cyberstratégie calquée sur la stratégie maritime devrait permettre de maîtriser tous les aspects qui lui sont nécessaires*". En effet, l'étude de la puissance britannique entre le XIXè et le début du XXè siècles montre comment, par des moyens essentiellement civils et secondairement militaires, le Royaume-Uni a imposé

[32] http://www.colsbleus.fr/articles/6515
[33] Voir à ce sujet le vif débat autour des contrats entre l'Education Nationale et, surtout, la Défense avec Microsoft : http://www.zdnet.fr/actualites/microsoft-et-ministere-de-la-defense-le-debat-sur-le-contrat-open-bar-fait-son-retour-39852820.htm
[34] http://bfmbusiness.bfmtv.com/hightech/vaste-cyberattaque-en-cours-dans-plusieurs-pays-contre-des-entreprises-et-des-institutions-1196008.html

matériel, normes et course à l'innovation. En quelque sorte nous avons là un parallèle à faire avec la maîtrise du software, du hardware et des normes (celles de la *Silicon Valley*) imposées aujourd'hui par les USA. La maritimisation du cyberespace est donc une piste porteuse de grands espoirs quant à une véritable réflexion stratégique.

C - Le cyber comme matrice des modifications de la guerre ?

Début 1968, alors que l'offensive du Têt organisée par le Vietcong et des unités du Vietnam du Nord était foudroyée par les Etats-Unis et les forces de **Pham Quoc Thuan**, la guerre du Vietnam entrait dans une phase décisive. *Têt Mau Than* avait été une cinglante défaite pour la RDV ; pour les USA, la défaite politique était tout aussi certaine et, d'un point de vue stratégique, la porte ouverte à une défaite dans cette guerre. Les seconde et troisième vagues d'attaque contre Hanoï transformèrent la défaite du Nord en désastre mais, pour Washington, coupé de son opinion publique et, plus généralement, du soutien de ses alliés occidentaux, le bilan était pire[35].

Clausewitz[36], plus cité que lut, a entre autre défini la Guerre comme un moyen d'action du Politique. Oublier ce principe fondamental et l'on passerait à côté des causes de la défaite américaine au Vietnam. Dans les démocraties occidentales, il est impossible de vaincre ou de s'engager avec quelque chances de réussites dans un conflit sans disposer d'une solide base populaire. Si le peuple ne soutien pas l'effort de guerre, fût-il modeste dans le cadre d'une OPEX, la guerre ne peut être gagnée. Quel est le lien entre le Vietnam des années 60 et le cyberespace du début du XXIè siècle ? Encore une fois tout est question de temps long, d'inerties et de mises en perspective.

En 2005 sous la plume de **Frank Hoffman** et **James Mattis** (*Future warfare : The Rise of Hybrid Wars*, Proceedings, vol.132) était défini le concept de "***guerre hybride***". Selon cette approche qui se voulait novatrice, il s'agirait d'une guerre irrégulière complexe dans laquelle des acteurs non-étatiques et étatiques usent d'armes conventionnelles aussi bien que de terrorisme ou de tactiques irrégulières[37]. En réalité cette approche se situe dans la droite ligne d'une réflexion amorcée dès les années 1970 en RFA, Norvège, France et USA autour de stratégies alternatives. En 2013 le Livre Blanc de la Défense citait explicitement ce concept comme grille de lecture majeure pour les conflits à venir[38]. Quel lien peut-on faire avec le cyberespace ?

---

[35] A ce sujet lire l'excellente mise à jour de John Prados, *La guerre du Viêtnam*, Perrin 2011
[36] Carl von Clausewitz, *Vom Kriege*, 1832

[37] Pour une analyse approfondie se référer au travail de Elie Tenebaum : https://www.ifri.org/fr/publications/enotes/focus-strategique/piege-de-guerre-hybride#sthash.Jfar6oyI.dpbs
[38] Livre Blanc Défense 2013

La guerre hybride bouscule les certitudes tel l'apex occidental entre contre-guérilla, contre-insurrection et opérations aériennes développé entre autres depuis la Guerre d'Algérie et celle du Vietnam[39]. En effet, la révolution technologique qui accompagne l'épanouissement du cyberespace fait passer un véritable saut qualitatif aux adversaires irréguliers. Les drones sont ainsi peut coûteux et utilisés par **DAESH** pour le renseignement comme pour la capacité de vecteur de charge anti personnelle. En Ukraine, en 2014, les forces loyalistes ont été décimées dans leur parc d'artillerie par l'utilisation d'un virus exploitant une faille du système *Android* de localisation des cibles et batteries. Les terroristes islamistes usent massivement d'internet pour diffuser leur propagande, pour détourner les images, pour intoxiquer les opinions publiques, comme la Russie a pu le faire dans l'affaire ukrainienne. L'hybridité modifie dans ce sens la guerre. La complexité des enjeux, des acteurs, rend nécessaire un temps de réflexion et de mise en perspective incompatible avec une information de la population reposant sur la masse de données, le zapping, l'émotion et donc la simplification. Ici, en réalité, rien de nouveau ; c'est par le divorce avec son opinion publique que les USA ont perdu politiquement, et donc stratégiquement, le Vietnam en 1968, sans internet. Le cyberespace agit comme un facilitateur de trouble mais utilise des logiques déjà éprouvées en stratégie. La dérégulation est un défi posé par une mise en scène sur internet d'exactions contraires au droit humanitaire et international. La *glocalisation* liée aux technologies de l'information et de communication permet de bâtir une véritable stratégie d'influence vis à vis des opinions publiques, à l'échelle mondiale, en se jouant totalement des contrôles aux frontières, et en tapant sur le point faible de l'Occident.

Dans ce sens, le cas du terrorisme est éclairant. Utiliser le mot guerre à propos du terrorisme est naïf et simplificateur. La "*Global War on Terror*" défini par l'administration **Bush** après les attentats du 11 septembre 2001 s'est avérée être un échec car, simpliste, elle ne prenait pas en considération la complexité des matrices du terrorisme[40]. Ce dernier repose sur l'effet de sidération, de peur à diffuser dans la société afin d'obtenir des décisions politiques allant dans le sens de la cause défendue. Il y a donc une véritable mise en scène liée aux médias. Il faut montrer pour terroriser. Dans nos démocraties se pose donc la question de l'image ; faut-il montrer et donc alimenter la peur ? Faut-il cacher et donc alimenter les théories, très en vogue chez les adolescents, du complot. Ou ne faudrait-il pas, selon l'exemple israëlien cité dans une interview pour Diploweb par **Gérard Chaliand[41]**, se contenter de citer les faits sans passer des heures à montrer des familles torturées par la douleur de la perte de proches ? Mais dans cette logique encore faudrait-il aussi

[39] https://www.cairn.info/revue-strategique-2009-1-page-357.htm
[40] https://www.cairn.info/revue-internationale-et-strategique-2006-3-page-7.htm
[41] https://www.diploweb.com/G-Chaliand-Irak-et-Syrie-quelle-situation-geopolitique-et-strategique.html

couper le canal des images via internet, ce qui est contraire à nos principes démocratiques du droit à l'information. C'est aussi par le cyberespace que les terroristes peuvent recruter ou se financer via le *crowdfunding* par exemple. De facto la maîtrise du cyberespace est un enjeu sécuritaire majeur.

Le cyber accompagne donc les modifications de la guerre sans en être la cause unique. Rappelons que le terrorisme fut un problème que les légionnaires romains rencontrèrent en Palestine au Ier siècle ...

Conclusion

Il est clair que le champ de bataille traditionnel s'est élargi au cyberespace. Les Etats dans leur quête d'influence, dans leur stratégie de pouvoir, usent de tous les moyens disponibles et en perpétuelle dilatation pour tenter de contrôler ce corps fluide. Le phénomène cyber démontre que le cycle offensif/défensif va pour le moment dans la victoire provisoire de la lance sur le bouclier. Ces logiques permettent de remettre au goût du jour des réflexions anciennes, car les inerties sont profondes, mais oblige aussi à penser des réponses adaptées à nos besoins et moyens dans une course mondiale qui semble devoir accélérer.

Ludovic Chevassus, 3 juillet 2017

Bibliographie de base

Ouvrages généraux sur la géopolitique et la stratégie

Hervé Coutau-Bégarie, *Traité de stratégie*, Paris, Economica, 2011

Gérard Chaliand et Arnaud Blin (dir), *Histoire du Terrorisme: De l'Antiquité à Daech*, Paris Fayard, 2015

Hervé Coutau-Begarie Hervé et Martin Motte, *Approches de la géopolitique*, Paris, Economica, 2015 (2è édition)

Stéphane Taillat, Joseph Henrotin, Olivier Schmitt, *Guerre et stratégie*, Paris, PUF, 2015

Olivier Zajec, *Introduction à l'analyse géopolitique : Histoire, outils*, Paris, Editions du Rocher 2016 (3è édition)

Ouvrages relatifs au "Cyber"

Daniel Ventre (dir), *Cyberguerre et guerre de l'information*, Paris, Lavoisier, 2010

Olivier Kempf, *Introduction à la Cyberstratégie*, Paris, Economica, 2012

Bertrand Boyer, *Cyberstratégie, l'art de la guerre numérique*, Paris, Nuvis, 2012

Bertrand Boyer, *Cybertactique : Conduire la Guerre Numérique*, Paris, Nuvis, 2014

Laurent Bloch, *L'Internet, vecteur de puissance des États-Unis ? Géopolitique du cyberespace, nouvel espace stratégique*, éd. Diploweb 2017

Revues

«TERRORISME - Organiser une riposte efficace» (2016, avril-mai.). DSI, no 47

«OPERATIONS TERRESTRES - La nouvelle donne» (2016, juin-juillet.). DSI, no 48

«CYBERGUERRE - L'heure de l'action» (2017, février-mars.). DSI, no 52