PROGRAMME ASIE

LE CYBERESPACE ET LE NATIONALISME CHINOIS : Le levier d'une grande puissance numérique

PAR **Emmanuel MENEUT**

DR. DE L'INSTITUT CATHOLIQUE DE PARIS,
CHARGÉ D'ENSEIGNEMENT

FEVRIER 2017

ASIA FOCUS #17

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

RÉSUMÉ

En résumé, nous explicitons la propriété de la situation décisionnelle associée à l'émergence d'une nouvelle arme. Ensuite, nous examinons le cas des cyberarmes qui introduisent une imprédictibilité structurelle à laquelle sont confrontés les dirigeants politiques. Celle-ci rend caduc la mise en place d'un régime de cybersécurité par des normes, elle conduit à un ordre international anarchique ou l'utilisation des cyberarmes est une pratique quotidienne en temps de paix ou de guerre. Dans ce cadre décisionnel, le levier de mobilisation sociale des ressources humaines nécessaires à la cyberguerre est un enjeu stratégique. La nature anarchique du cyberespace conduit à recourir à un levier classique de mobilisation : le nationalisme. La Chine illustre particulièrement cette situation à travers les spécificités de son nationalisme et de sa puissance numérique.

A la veille de son départ, le président Obama a attiré l'attention de son successeur D. Trump sur l'importance du cyberespace qui a déjà mobilisé une part importante de son énergie avec la création du *Cyber command* sous son administration en 2010 : « Il est temps pour la prochaine administration de prendre ce problème à bras-le-corps pour s'assurer que le cyberespace puisse rester un catalyseur pour la prospérité, l'innovation et le changement, aussi bien aux Etats-Unis que dans le reste du monde. » (ASSOCIATED PRESS, 3/12/2016) Dans un espace public récemment conditionné par les fuites de courriels du parti démocrate pendant la campagne présidentielle, cette déclaration amplifie les conclusions d'un rapport d'une commission d'experts, dont la principale recommandation est la création d'un poste de conseiller présidentiel et d'ambassadeur pour promouvoir des normes globales et structurer l'ordre international à venir.

Ce nouveau défi provient de l'émergence du cyberespace. C'est une rupture stratégique car c'est un nouveau théâtre d'opération qui modifie les caractéristiques de la rivalité entre les grandes puissances. C'est un nouvel environnement décisionnel qui nécessite des ressources humaines pour lesquelles le nationalisme devient un outil de mobilisation social efficace du large éventail d'expertises humaines, du cybersoldat au spécialiste d'entreprise, comme l'illustre la puissance numérique chinoise. A partir d'une mise en perspective historique nous identifions les caractéristiques du phénomène observé, la notion de rupture stratégique associée à l'émergence d'une nouvelle arme. C'est la prise de décision sous un voile d'ignorance induit par une rupture technologique. Puis, quelques exemples nous permettent de cerner la variable critique nécessaire pour tirer profit d'une innovation, c'est l'existence d'un levier de mobilisation sociale : le nationalisme qui permet la clôture de l'espace social dans une situation décisionnelle sous un voile d'ignorance. Ainsi, nous analyserons le rôle du nationalisme chinois et son apport pour tirer parti de cette nouvelle opportunité stratégique offerte par le développement du cyberespace et l'avantage stratégique de grande puissance numérique qu'il confère à la Chine. Les entreprises et les associations, les acteurs chinois non étatiques du cyberespace jouent un rôle clé dans la constitution de cette puissance. Cette émergence de nouveaux acteurs nous conduit à une redéfinition du rôle de l'Etat dans la cyberpaix.

CARACTÉRISTIQUES DES RUPTURES STRATÉGIQUES INDUITES PAR DE NOUVELLES ARMES

Nous allons définir une rupture stratégique par l'utilisation d'un nouveau système d'arme, une innovation technique, conduisant à un changement profond de la

doctrine d'emploi, de la stratégie et du type de conflit. Dans l'histoire militaire, nous prendrons trois exemples afin de cerner cette notion :

- **L'avantage de l'arc long est révélé à la bataille de Crécy en 1346. Son emploi permet de créer une pluie de flèches qui s'abat sur les chevaux de la cavalerie ce qui réduit à néant sa force de charge. Pour obtenir ce résultat il faut changer l'ordre de bataille. Les archers sont placés en première ligne à la place de la cavalerie. De plus, il faut posséder un nombre important d'archers efficaces, ce qui nécessite un levier de mobilisation sociale pour assurer la formation des archers dès le plus jeune âge et la disponibilité permanente de ressources humaines spécialisées.**

- **La mitrailleuse Gatling et son apparition pendant la guerre de Sécession, le modèle de Reffy pendant la guerre de 1870 et la mitrailleuse britannique Maxim qui devient une arme encore plus redoutable sont un nouvel armement qui modifie complètement la stratégie de la guerre. L'accroissement de la cadence de tir de la mitrailleuse, passant de 160 à 300 coups minute et la facilité du rechargement remet en cause la doctrine de l'offensive à outrance. Le feu ininterrompue brise les élans offensifs de l'infanterie au début de 1914 et conduit à l'échec des plans de campagnes initiaux des belligérants qui s'installent dans une guerre de défense des positions dont le bilan humain est terrifiant : une moyenne de 900 morts par jour. (CONRAD, 2015) Cette rupture technologique oblige les états-majors à passer d'une stratégie de mouvement pour encercler l'ennemi à une guerre d'attrition nécessitant la mobilisation totale de la société. Il ne s'agit pas de développer un corps d'élite pour l'utilisation de cette arme comme pour l'arc long. En effet, ce n'est pas la difficulté de l'utilisation de la mitrailleuse qui est déterminante dans ce type de conflit. (MONTBRIAL & KLEIN, 2000) Il faut un levier de mobilisation sociale des ouvriers et des ouvrières pour obtenir la capacité à produire en masse des mitrailleuses et les utiliser le long d'un front continu de plusieurs centaines de kilomètres.**

- **Autre exemple, l'arme nucléaire : « La capacité de destruction de l'arme nucléaire est telle qu'elle tend à rendre la guerre absurde, puisqu'elle entraine la mort assurée des deux combattants. » (RANOU, 2013) La guerre repose alors sur une rationalité coût/bénéfice qui devient structurante sur les relations internationales. Il peut y avoir des guerres limitées (guerre par proxy) mais la priorité est de garder le contrôle de l'escalade avant de faire plier la volonté de l'adversaire. L'arme nucléaire induit le développement d'une culture du calcul stratégique, par exemple aux Etats-Unis avec le développement des centres de recherche tel que la RAND Corporation, etc. afin de développer cette intelligence stratégique. Un levier de mobilisation social est nécessaire pour mettre en place un capital social,**

un groupe de spécialistes en réseaux qui produit des connaissances stratégiques utiles aux décideurs confrontés à ce nouveau type de conflit.

Une innovation de systèmes d'armes peut induire une rupture d'ordre tactique, stratégique, géopolitique. "Le fait qu'une mutation des armements, des méthodes de combat et de la violence de guerre a eu lieu au XIXème siècle ne signifie pas pour autant qu'elle ait été comprise ou qu'elle ait permis d'anticiper ce que serait la Grande Guerre. Malgré les rapports des observateurs militaires lors de la guerre russo-japonaise ou des guerres balkaniques, le déluge de feu de 1914 a pris les contemporains largement par surprise." (CABANES, 2013) Si l'innovation n'est pas prédictible, la nécessité d'évaluer son impact est primordiale dans la régulation des rapports de force. L'incapacité des puissances européennes à comprendre les implications du développement de la mitrailleuse ou celles concernant la Blitzkrieg a eu des conséquences tragiques pour l'ensemble ou pour l'un des acteurs de ces conflits. (FRIESER, 2003) La caractéristique centrale de ces exemples est le levier de mobilisation social nécessaire pour tirer parti de l'émergence d'un nouveau système d'arme, formation des archers dans la population villageoise anglaise, la mobilisation des ouvriers et ouvrières des industries d'armement pour la production de mitrailleuses, la formation de spécialistes des armes atomiques et de la théorie des jeux dans les centres de recherche.

L'enjeu du cyberespace est de même nature que celui induit par la rupture technologique des armes nucléaires à l'aube de la Guerre froide : « Comme lors de toutes les innovations technologiques, il sera difficile de résister à la tentation de profiter de ce nouveau domaine pour prendre un avantage stratégique. » (KISSINGER, 2014). Cette tentation se concrétise donc par un processus de mobilisation des ressources humaines nécessaires à la mise en œuvre des cyberarmes dans le cyberespace.

Plus précisément, à l'origine du défi stratégique de la mobilisation sociale des ressources, il y a cette notion de rupture technologique d'une nouvelle arme qui introduit l'imprévisibilité au cœur de l'interaction stratégique entre deux acteurs.

Dans une situation classique, deux acteurs A et B interagissent dans un environnement aléatoire mais prédictible. Dans un environnement prédictible l'acteur A a une visibilité sur B qui lui permet de modéliser ses comportements possibles. Par exemple, s'ils sont au nombre de deux, l'acteur A peut les représenter par un pari sur une loterie Pile ou Face. Dans un environnement transparent, si le comportement de B est équiprobable alors A peut choisir une pièce non truquée pour modéliser la situation décisionnelle. Supposons que A représente l'incertitude quant au comportement de B par une pièce non truquée avec l'alternative Pile (P) ou Face (F). Dans un tel environnement, l'acteur A peut

donc représenter sa croyance quant au comportement de B par la distribution de probabilité p(P) = p(F) = 0.5.

Si les deux acteurs signent un accord à travers une organisation internationale qui stipule que les gains pour A soient distribués selon la règle suivante : si le comportement de B est P alors A gagne $60 tandis que si le comportement de B est F alors A perd $-30. Dans ce cas, le gain espéré de A est $15 et il a intérêt à coopérer avec B en respectant cet accord. Etant donné un environnement prédictible, il y a une connaissance commune entre A et B, A peut se mettre à la place de B et réciproquement pour trouver une décision pour chacun qui soit telle qu'aucun ne puisse individuellement mieux faire si l'autre ne dévie pas de sa décision.

Un cyberespace prédictible repose sur une technologie connue, partagée et stable ; le critère de choix des acteurs porte exclusivement sur l'optimisation des coûts et des gains des entreprises et sur la non-ingérence politique des Etats, alors il est possible de construire un accord afin de partager les bénéfices de la révolution numérique de façon pacifique, car le comportement aléatoire de chacun sera prédictible.

Au contraire, dans un environnement imprévisible, le comportement de B n'est pas modélisable par A. Plus précisément, l'acteur B peut élaborer une stratégie de double commande. D'une part, B tient un discours coopératif, il annonce qu'il suit les accords signés, il adhère à la structure des gains de l'accord. D'autre part, grâce aux cyberarmes qu'il a introduit dans les infrastructures critiques de l'acteur A (« back door », « trapdoor », « logicbomb ») et au cyberespionnage il modifie l'environnement de l'acteur A et la probabilité réelle de P et F. Nous pouvons ainsi représenter le comportement de B par celui d'un joueur muni d'un dé, lorsque l'as sort il annonce P à A sinon pour 2, 3, 4, 5 et 6 il annonce F (DUBOIS, PRADE, & SMETS, mai 1996). La nouvelle distribution de probabilité est p(P) = 1/6 et p(F) = 5/6. Dans le cadre de l'accord signé, c'est une perte moyenne de $-15 pour A. L'acteur A n'a pas les moyens de détecter cette situation perdante car l'acteur B a modifié l'environnement informationnel de A.

Dans un environnement où le cyberespace est caractérisé par des ruptures technologiques permanentes, l'incertitude relative au comportement de B n'est pas une probabilité d'un phénomène aléatoire, c'est un voile d'ignorance qui n'est pas probabilisable. En effet, une rupture technologique se caractérise par une courbe en « S ». Lorsqu'une rupture fonctionne, elle se diffuse et se généralise rapidement à l'ensemble du cyberespace, de la même façon que l'arc long, la mitrailleuse ou la bombe atomique se sont imposés. Le basculement entre la phase d'incubation de la rupture et la phase de diffusion est complètement indéterminé.

En effet, dans le cyberespace, chaque innovation offre à l'acteur B la possibilité permanente de produire une cyberarme pour le nouveau cyberespace qui lui permettra de prendre le dessus sur A en cas de conflit ouvert.

La particularité des ruptures technologiques du cyberespace c'est la modification de l'environnement informationnel des acteurs. A chaque nouvelle rupture technologique dans le cyberespace, l'acteur B se voit offrir la possibilité de renverser le rapport de force avec A en modifiant non pas les gains issus des accords, mais la croyance de son adversaire à travers la modification de son environnement informationnel. Sans modifier la règle de décision précédente, l'acteur A est toujours convaincu qu'il a intérêt à jouer avec B pour un gain espéré de $15 alors que c'est une perte moyenne de $-15 car B a modifié son comportement sans conduire l'acteur A à changer sa distribution de probabilités. Cette possibilité est offerte à B par l'intermédiaire de ses capacités cybernétiques de modification de l'environnement informationnel de A.

Dans un environnement modifié par une rupture technologique l'acteur A ne peut pas prédire le comportement de son adversaire B. Dans un environnement imprévisible, il a une connaissance incomplète. Il doit faire l'hypothèse qu'il va parier sur une pièce équilibrée (principe de raison suffisante dans un contexte de "fog of war"). Si la règle de distribution des gains reste la même, dans notre exemple, l'acteur A a donc toujours intérêt à jouer avec son adversaire. Malheureusement, grâce aux ruptures technologiques l'acteur B peut modifier l'environnement informationnel de A en le plaçant dans une situation perdante (situation de Dutch book).

Plus précisément, le cyberespace a introduit les vulnérabilités 3A : abordable, accessibilité, anonymat. Par exemple, le Darknet est constitué par une collection de pages non indexées donc impossible à trouver grâce aux moteurs de recherche. Ces pages sont accessibles à l'aide du logiciel TOR qui brouille l'adresse IP de l'utilisateur et il procure un parfait anonymat et un accès à des contenus qui ne répondent à aucune loi ce qui permet le trafic d'armes et d'argent. Ainsi, les cyberattaques sont permanentes, autant en temps de paix que de guerre, elles sont difficiles à attribuer, le cyberespace devient donc un environnement très similaire à l'état de nature théorisé par Hobbes. (KISSINGER, 2014)

Dans un environnement imprévisible un décideur ne peut pas construire la distribution de probabilité sur les scenarii anticipés de l'adversaire. Même s'il suit une règle de décision rationnelle, il ne peut pas éviter d'être dans une situation sûrement perdante. Une rupture technologique introduit un voile d'ignorance sur les situations décisionnelles des acteurs et ils deviennent imprévisibles, ils ont les moyens de modifier l'environnement stratégique.

LE CYBER ESPACE : UN ENVIRONNEMENT PORTEUR DE RUPTURES QUI DIFFUSE L'IMPRÉVISIBILITÉ

Plus précisément, ce ne sont pas les cyberarmes qui sont des ruptures mais le cyber espace qui est leur vecteur. La caractéristique des cyberarmes en tant que programme autopropageable repose sur le principe du détournement du contrôle de la machine de Turing dans la mémoire de laquelle il se trouve. La première cyberarme date de 1982 alors qu'Internet n'était qu'un prototype et le cyberespace inexistant. Le vecteur de cette cyberarme était humain comme pour l'attaque de la centrale nucléaire iranienne de Natanz par Stuxnet. Si chaque cyberarme est spécifique à sa cible, son principe est toujours celui du « vol du contrôle d'une machine de Turing ». Depuis, les cyberarmes ne présentent pas de nouvelles innovations fondamentales. Les fonctions d'une cyberarme évoluent, elles deviennent plus complexes, leurs coûts de construction par composants diminuent, mais il n'y a pas de changement du paradigme.

Aujourd'hui, la rupture provient de la numérisation des infrastructures d'une société. Ce qui change ce ne sont pas les armes avec l'apparition de nouvelles cyberarmes, c'est l'environnement. Ce qui prolifère ce ne sont pas les armes, ce sont les cibles, l'origine de la vulnérabilité c'est le cyberespace. Il n'est pas un milieu naturel, il est entièrement d'origine sociale. Le cyberespace, ce sont des millions d'ordinateurs, de machine de Turing, connectés entre eux. La description faite par H. Kissinger dans son ouvrage « World order » pour ce phénomène repose sur les termes utilisés pour décrire un phénomène social non linéaire sous la forme d'une « révolution numérique » qui conduit à la prolifération des cibles des cyberattaques au point où toutes les activités humaines sont désormais vulnérables : « Le nombre d'appareils connectés à Internet étant dorénavant d'environ 10 milliards (il devrait même passer à cinquante milliards d'ici à 2020), nous sommes menacés par un « Internet des choses », ou un « Internet de tout ». » (KISSINGER, 2014) Cette connectivité facilite l'utilisation des cyberarmes. Ainsi, un logiciel espion a été identifié sur des Smartphone chinois (700 millions de mobiles), il permet de collecter des informations sur les déplacements de l'utilisateur, le contenu et les destinataires de ses messages. (TRUJILLO, 17/11/2016) Ce qui est variable dans cette configuration c'est bien le cyberespace, c'est l'environnement, le théâtre d'opération, ce n'est pas l'armement.

Le cyberespace est un système de communication non centralisé. A l'origine de l'innovation du cyberespace il y a le défi de résister à une attaque nucléaire qui conduit à la mise au point d'une architecture distribuée. Chaque nœud du réseau possède suffisamment de capacités et ils sont tous aussi efficaces les uns que les autres pour assurer la fonction de circulation des messages dans le réseau. La destruction d'un nœud n'altère pas la qualité de la communication entre deux ordinateurs (modulo la distinction entre ordinateur et serveur comme l'a illustré

la récente attaque sur la société DYN gestionnaire de DNS le 21 octobre dernier (LE PARISIEN, 27/10/2016,)). Une architecture distribuée de réseaux de communication est donc résiliente face à une attaque nucléaire.

La fiabilité et le faible coût de cette architecture ont conduit au déploiement des autoroutes de l'information depuis les années 1990 qui assurent la connexion de tous les réseaux existants entre eux. La mise au point de la navigation par hyper lien a conduit au cyberespace qui permet l'utilisation de ce type de réseaux de communication par n'importe quel utilisateur sans compétences particulières. La rapidité et l'étendu de ce phénomène est expliqué par la « loi de Moore », le doublement des capacités de calcul des ordinateurs tous les deux ans depuis le 1er microprocesseur d'INTEL en 1972 et « la loi des réseaux » qui conduit à l'interconnexion de tous les réseaux afin de permettre la création de valeur à travers les échanges dans le cyberespace. C'est bien la nature non linéaire de ce phénomène qui retient l'attention du dirigeant et qui caractérise la problématique de sécurité auquel il est confronté : « La communication à travers le cyberespace entre ses nœuds, dont la prolifération s'opère à un rythme exponentiel, est presque instantanée. » (KISSINGER, 2014) p 322

L'enjeu économique devient l'extension du cyberespace à l'ensemble des activités humaines. Plus précisément, la connexion des infrastructures de la société sachant que le cyberespace, s'il résiste à une attaque nucléaire, il n'est pas résilient face à une cyberarme. Par conséquent, l'enjeu politique associé est celui de sa sécurisation par l'Etat afin de garantir la sécurité des infrastructures. Selon H. Kissinger, le constat qui s'impose aujourd'hui aux dirigeants politiques est : « Notre époque se distingue cependant par la rapidité d'évolution de la puissance informatique et l'invasion de toutes les sphères de l'existence par la technologie de l'information. » (KISSINGER, 2014) p322

Le cyberespace, résultat de volonté humaine, est caractérisé par son extension rapide à toutes les activités d'une société. La spécificité de cet environnement c'est son évolution permanente sous la forme de ruptures qui se diffusent à toutes les activités humaines. Elles induisent un voile d'ignorance sur les interactions stratégiques entre les grandes puissances numériques.

Dans le cyber espace il y aura toujours un acteur qui produit une cyberarme pour cibler chaque nouvelle machine de Turing : serveurs, ordinateurs, tablettes, téléphones mobiles, voitures, centres de contrôle etc. dont l'accès est rendu très facile par sa connexion au cyberespace. L'emploi de cette cyberarme modifiera les rapports de force. Par conséquent, le cyberespace est un environnement imprévisible qui positionne les acteurs étatiques sous un voile d'ignorance permanent. L'extension du cyberespace à l'ensemble des activités humaines rend possible en permanence et de façon imprévisible pour un adversaire de « détruire une infrastructure vitale, en bénéficiant d'un anonymat presque total. Des réseaux

électriques pourraient être mis en surtension et des centrales électriques hors d'usage par des actions entreprises exclusivement à l'extérieur du territoire physique d'une nation. » (KISSINGER, 2014)

LES CONSÉQUENCES DE L'IMPRÉVISIBILITÉ SUR L'ORDRE INTERNATIONAL

Ainsi, pour les acteurs de cette évolution permanente du cyberespace, les GAFA, la sécurité est un défi continu associé à un coût, il faut donc le réduire au maximum et l'Etat, l'acteur qui porte les processus de sécurisation, est souvent perçu comme un tyran intrusif potentiel dont il faut limiter le rôle pour ne pas nuire à la réputation d'intégrité morale de la marque. La globalité du cyberespace nécessiterait la mise en place d'un régime international de cybersécurité entre ces acteurs. Malheureusement, le concept de cybersécurité collective a le même défaut que son prédécesseur la sécurité collective. Selon H. Kissinger : « La communauté de force [la SdN] dont parlait Wilson remplaça la rigidité des alliances [qui avaient conduit à la WWI] par l'imprévisibilité [qui conduit à la WWII] » (KISSINGER, 2014) p.249

En effet, un régime nécessite d'établir des normes : « La sécurité collective cherche à régler le problème de la violation de normes. Dans la mesure où leur définition est sujette à des interprétations divergentes, le fonctionnement de la sécurité collective est imprévisible » (KISSINGER, 2014) p.250 Au contraire d'une alliance qui repose sur la perception commune d'une menace et qui conduit à des comportements explicites, la sécurité collective doit répondre à la violation d'une règle internationale au cas par cas. (KISSINGER, 2014) Ainsi, pour appliquer une norme, il ne faut pas que certains acteurs puissent pratiquer l'espionnage et la duplicité pour se concentrer sur leurs intérêts en priorité. Ils doivent pouvoir tous s'unir lorsqu'une norme est violée en faisant abstraction des résultats particuliers à la situation sur leurs propres intérêts. Le cas de l'Estonie en 2007 a bien montré les limites de la communauté de sécurité américano-européenne de l'OTAN. Les pays membres, hormis l'Estonie, ont refusé d'invoquer le titre V du Traité de l'Atlantique Nord afin de répondre à la cyberattaque russe. Chaque puissance est restée guidée uniquement par son intérêt national et le rapport de force existant. De même, lors de la cyberattaque nord-coréenne contre le film « The interview » de Sony Picture Entertainement le président Obama avait initialement dénoncé celle-ci comme une agression contre le droit à l'expression de la Constitution américaine. Puis, elle fut requalifiée en acte de cybervandalisme afin d'éviter une escalade de la tension vers une intervention armée conventionnelle contre un pays « voisin » de la Chine.

Un régime de cybersécurité qui repose sur des normes sous un voile d'ignorance permanent induit par les ruptures technologies du cyberespace ne permet pas de

réduire l'imprévisibilité sur le comportement des acteurs et ce sont donc les rapports de force qui prédominent. De plus, des alliances, par exemple des démocraties contre les régimes autoritaires, ne constituent pas une réponse adaptée au caractère global de la révolution numérique. Cette situation est permanente, elle est intrinsèque au cyberespace, c'est une structure de la société internationale.

En résumé, comme toute innovation technologique, le cyberespace et son développement exponentiel induit une incertitude radicale sur les capacités réelles des adversaires. Les acteurs sont donc en permanence dans une situation de prise de décision sous un voile d'ignorance qui rend imprévisible l'interprétation et la réaction à une cyberattaque ou l'intention qui prévaut à l'origine d'un tel comportement. L'interprétation des normes s'effectue sous un voile d'ignorance provenant de l'évolution de la technologie du cyberespace qui offre la possibilité permanente de renverser les rapports de force.

Enfin, dans le cyberespace, l'adversaire est invisible, les acteurs sont dans une situation d'anarchie structurelle. Il est donc très difficile d'établir des normes qui ne reposent en dernière instance que sur des rapports de force induit par les capacités offensives et défensives de chaque acteur. De plus, les cyberarmes favorisent l'attaque au détriment de la défense, dans un tel univers anarchique, la guerre ou le recours au cyberarmes est une activité quasi permanente.

Si les normes ne sont pas une solution pour établir la sécurité dans le cyberespace, elle sera donc le résultat « d'un mélange de dissuasion et de retenue mutuelles, associés à des mesures destinées à éviter une crise due à une mauvaise interprétation ou à une erreur de communication. » (KISSINGER, 2014), c'est un retour à la Guerre froide entre les grandes puissances numériques de la scène internationale. Plus précisément, les cyberarmes sont un outil de la diplomatie coercitive où la guerre est latente et dont l'espionnage et la guerre de l'information sont les caractéristiques saillantes du quotidien des relations internationales. La guerre à grande échelle est alors un échec de la diplomatie coercitive.

Face à ce changement stratégique le levier de mobilisation social est la variable critique dans la constitution de la puissance numérique d'un pays.

En effet, par rapport à d'autres systèmes d'armes comme les mitrailleuses, la spécificité des cyberarmes c'est l'expertise humaine nécessaire à leur fabrication. Elle constitue le capital social des réseaux critiques au sein des armées et des entreprises qui fait la différence entre deux Etats de façon similaire à la rupture

de l'arc long et des archers anglais. On ne compte pas le nombre de cyberarmes comme les missiles atomiques pour évaluer la puissance numérique d'un pays ; mais, le nombre de cyberguerriers quel que soit leur statut officiel ou non, étatique ou non. L'enjeu politique est donc quel acteur doit entretenir et mobiliser les cyberguerriers en charge de la cyberguerre ? l'Etat ou les entreprises

LE RÔLE DU NATIONALISME EN CHINE

Le cyberespace induit un processus de décision sous un voile d'ignorance. En fonction de ses objectifs, l'État doit pouvoir choisir les moyens d'action étant donnée la situation à laquelle il est confronté. Ce levier d'action doit permettre de mobiliser un large éventail de compétences et de ressources humaines dans le cyberespace : des soldats, des pirates, des mercenaires, des ingénieurs, des techniciens. Sa fonction, c'est la coordination de ressources mobilisées déjà dotées d'une expertise pour affronter une situation donnée et mener à bien une cyberattaque. Ce levier actionne ce qui constitue le capital social d'un pays dans le secteur numérique, sa puissance numérique. Nous allons aborder cette problématique à travers le nationalisme comme facteur de mobilisation sociale et plus particulièrement le nationalisme de la puissance numérique qui est porteuse du plus grand défi pour le statu quo : le nationalisme chinois.

Suivant l'hypothèse formulée par J.P. Cabestan : « Le quasi-monopole exercé par les élites dans la formation du nationalisme et la faible interaction entre celles-ci et le reste de la société qui, structurée autour d'obligations familiales et personnelles, demeure, sauf en période de crises majeures, relativement hermétique à cette idéologie et surtout à sa traduction dans l'action.[…] Cette spécificité favorise une plus forte manipulation du nationalisme par les élites, et en particulier par celles qui interagissent de manière privilégiée avec le pouvoir. » (CABESTAN, 2005) Ainsi, selon J.P. Cabestan, le nationalisme chinois, la loyauté des acteurs du cyberespace à l'égard de l'Etat et du PCC est un levier de l'Etat actionné selon ses intérêts de politique étrangère. Les manifestations antijaponaises du printemps 2005, notamment à l'occasion des accrochages maritimes autour des îles Senkaku et leur nationalisation par Tokyo a illustré le rôle du nationalisme comme outil de mobilisation pour atteindre un objectif stratégique, sur la scène internationale, et affirmer un rapport de force régional. (CABESTAN, 2005) Ce levier est-il efficace pour les acteurs du cyberespace ?

Le nationalisme est une clôture de l'espace social qui permet de décider sous un voile d'ignorance pour une situation donnée qui est l'ami/ennemi. Ce levier permet de mobiliser les ressources nécessaires, cybersoldats, mercenaires, hackers ou experts d'entreprise afin d'atteindre ses objectifs stratégiques.

Plus précisément, les groupes de cybersoldats en charge du cyberespionnage sont le 3ème département de l'APL (APL-3) et le 4ème département (APL-4). L'APL-3 c'est 20 000 spécialistes du cyberespace. (FALIGOT, 2010) Ces services mènent une guerre d'intrusion permanente sur des sites à l'étranger. Plusieurs entreprises ou Etats ont été attaquées, le « Pentagon » en 2005 ou Mitsubishi et Sony. (FALIGOT, 2010) D'après Verizon, en 2013, 49% des campagnes de cyberespionnage provenaient de Chine et d'Asie. (LA TRIBUNE, Cyberespionnage, les Etats sont les plus grand pirates, 22 avril 2014) La Chine possède les moyens d'interceptions les plus important. (FALIGOT, 2010) Elle est le pays n°1 pour la mise en pratique des techniques de guerre de l'information. Récemment, les Etats-Unis ont inculpé 5 officiers de l'APL-3 pour des faits d'espionnage économique, perpétrés entre 2006 et 2014 à l'encontre de 6 sociétés américaines des secteurs de l'énergie nucléaire, solaire et de la métallurgie. (LA TRIBUNE, Cyberespionnage : la justice américaine inculpe des officiers chinois, 19 mai 2014) Les cybersoldats sont « naturellement loyal » à l'institution étatique et ils ne sont pas les seuls.

La justice américaine a condamné un hacker pour sa participation efficace à la cyberattaque de type Advanced Persistent Threat (APT) Titan Rain de 2008 à 2014 qui a permis aux cybersoldats chinois de pirater les données de nouveaux systèmes d'armes comme l'avion de chasse F35 et le Boeing C17. Il a fourni des notes de synthèse sur les technologies de rupture à cibler. Il a permis d'identifier les entreprises et les personnes clés à pirater. Ce hacker possède la nationalité chinoise et il admet avoir aidé l'APL contre un gain financier. (YAN & JIANG, (Juillet 2016),) C'est un mercenaire chinois.

Dernier exemple, les experts de l'entreprise chinoise Tencent Elite Keen ont récemment démontré leur capacité de cyberattaque sur la voiture automatique de l'américain Tesla, le modèle S, en prenant son contrôle à 12 km de distance. Le piratage de ce véhicule a été réalisé grâce à une borne WIFI malveillante d'une station de recharge. La faille était localisée dans le « browser » du véhicule utilisé par le conducteur. Cette équipe d'experts chinois est l'une des meilleures du monde, elle a déjà obtenu de nombreux succès sur des iPhone et des appareils Google/Android. (FOX-BREWSTER, 21/9/2016,) Leur exploit à l'encontre de produits américains n'a jamais été tenté à l'égard de leur équivalent chinois.

La Chine dispose ainsi d'un large éventail de cyberguerriers dans le cyberespace : les officiers de l'APL, les pirates rouges (red hacker ou honker) et les experts de cybersécurité à l'origine du piratage exemplaire de la Tesla. C'est la loyauté nationale qui permet à l'Etat d'utiliser ces ressources en fonction des besoins de la situation stratégique rencontrée. Selon Wang Zi, président de la Honker's Union of China qui compte de 8 000 à 80 000 membres : « Nous sommes des hackers patriotiques, mais nous sommes une organisation totalement civile. Nous évitons tout contact avec le gouvernement et nous ne sommes jamais payés par lui. » (IHS,

2016) Il est à la tête d'un cabinet de conseil en cybersécurité qui réalise des travaux pour les entreprises chinoises, surtout étatique.

A ce rôle primordial du nationalisme chinois pour mobiliser le capital social des acteurs du cyberespace au bénéfice de la politique étrangère nous devons aussi ajouter l'examen pratique de sa mise en œuvre.

Selon la théorie de Stein Rokkan, le processus historique de la formation des Etats s'est accompagné « de la création de frontières territoriales et d'affiliation concernant la loyauté des individus. Ces deux frontières, géographique et d'appartenance sociale sont couplées et elles entrainent une forclusion progressive des possibilités de sortie physique ou de défection nationale pour les individus, les acteurs sociaux et leurs ressources. Elle s'est accompagnée d'institutions capables d'assurer le maintien du système social et de la loyauté nationale. » (FERRERA, 2002)

Nous constatons cette clôture territoriale du cyberespace par l'intermédiaire des entreprises chinoises qui sont aujourd'hui des alter ego des acteurs américains : Baidu vs Google, Lenovo vs IBM, Huawei vs Cisco, etc. Elles sont aujourd'hui capables de mettre en place le « Great firewall » qui assure la sécurité intérieure chinoise dans le cyberespace. Le défi initial pour la Chine dans le cyberespace, c'est la sécurité de l'État face aux mouvements de l'opinion publique. Dès 1995, Jiang Zemin créa un organisme central pour les affaires du Web. De plus, 2 fournisseurs dépendants de l'Etat couvrent l'offre d'accès à Internet, China Netcom au nord et China Telecom au sud. En 1996, la China Internet Company élabore la Grande Muraille virtuelle d'un "China Wide Web" en circuit fermé. (FALIGOT, 2010) A cette époque, le nombre d'internautes chinois était de quelques milliers d'universitaires qui devaient s'enregistrer auprès du Ministère des P&T. 10 ans plus tard, leur nombre dépassait les 80 millions. Aujourd'hui, il y en a 457 millions. (TRAN DAI, février 2011) C'est une diffusion massive de la rupture technologique du cyberespace. Face à ce défi l'Etat chinois a su mettre en place un réseau de grandes entreprises et d'associations dédiées à sa sécurité. Les capacités de censure sont telles qu'en avril 2015, la censure chinoise s'est projetée de manière offensive dans le cyberespace avec l'attaque DDOS du réseau social Github. La faille utilisée provenait des certificats fournis par l'organisation China Internet Network Information Center censée garantir la sécurité des sites web accédés par les internautes.

Au fur et à mesure de l'évolution technologique l'Etat adapte ses moyens de sécurisation à travers les capacités des entreprises chinoises du secteur numérique.

C'est un ensemble de matériels et de logiciels déployés par des entreprises et des agences du renseignement pour contrôler le web et son accès par les internautes chinois sur le territoire. Cette frontière physique du cyberespace s'accompagne,

selon la théorie de S. Rokkan, d'un mécanisme de loyauté à l'égard des intérêts de l'Etat chinois et du PCC. En effet, c'est par l'intermédiaire des acteurs non étatiques, entreprises et groupes sociaux que la Chine a élargi ses capacités humaines. Ainsi, l'équipementier Huawei, $15 milliards de chiffre d'affaire, 60 000 employés, fondé en 1988 par un ancien officier de l'APL, Ren Zhengfei, compte de nombreux anciens des services de sécurité chinois au sein de ses équipes de direction. Cet acteur majeur du cyberespace est un concurrent direct de l'américain Cisco et sa loyauté à l'égard de l'Etat chinois est avérée. En 2009, Huawei a été désigné par les experts britanniques du GCHQ comme une menace pour la sécurité informatique du Royaume Uni.

Le cyber espace accroit la diffusion du pouvoir vers des acteurs non étatiques qui obtiennent de nouveaux moyens d'actions. Ceux-ci, les entreprises et les associations, se trouvent au cœur des leviers politiques des cyberarmes. Ainsi, la problématique propre de la cybersécurité devient : est-ce que la délégation de la sécurité aux entreprises chinoises et à leur loyauté offre des perspectives stratégiques nouvelles ?

LE CYBER ESPACE ACCROIT LA MONTEE EN PUISSANCE DES ACTEURS NON ETATIQUES

L'intensité de l'emploi des cyberarmes et des stratégies d'influences que nous observons actuellement trouve son origine dans la diffusion de ces capacités cybernétiques à des acteurs non étatiques qui sont partenaires des Etats. Cette diffusion provient du faible coût d'accès au cyberespace et de l'anonymat afférent.

En effet, le cyberespace permet d'atteindre l'opinion publique et de nuire aux activités économiques de l'adversaire qui sont deux objectifs stratégiques du soft power entre des rivaux politiques dans un contexte de société unipolaire où le hard power (les moyens diplomatico-militaires) sont l'objet d'un monopole de fait par la puissance américaine.

Ainsi, le cyberespace a permis la diffusion de capacités d'action des Etats vers les entreprises qui sont de fait les nouveaux acteurs de la cybersécurité. « Les entreprises qui rassemblent et contrôlent les données échangées par les utilisateurs ont des capacités d'influence et de surveillance supérieures à celles de beaucoup d'Etats contemporains et de puissances encore plus traditionnelles. » (KISSINGER, 2014) p323 La problématique stratégique pour les Etats est donc « faut-il s'abriter sous la protection des sociétés high tech ? » (KISSINGER, 2014) p326

Le régime chinois et le poids du PCC dans la gouvernance des grandes entreprises du secteur numérique répond par l'affirmative et elle semble positionner la Chine

comme une grande puissance de la révolution numérique alter ego des Etats-Unis. La cybersécurité est un sujet régulièrement à l'ordre du jour de la rencontre annuelle entre les deux grands.

Sur la scène internationale, la récente privatisation de l'ICANN qui administre le backbone et le système d'adressage au profit des entreprises du secteur numérique confirme cette tendance à la délégation de la cybersécurité vers des acteurs du secteur économique (LE FIGARO, 2016). L'enjeu devient la loyauté respective de ces entreprises et associations vis-à-vis de leur État de référence. L'articulation entre cybersoldat, hacker et les experts d'entreprises conduit à un élargissement de la sécurité du champ politique étatique vers les acteurs économiques avec la nécessité pour l'État de redéfinir son rôle au regard des capacités des entreprises. C'est la centralité de l'Etat qui est concernée et sa capacité de mobilisation des ressources humaines à travers le levier du nationalisme. Si l'Etat est celui qui peut légalement définir les normes de la cybersécurité assurée par les entreprises il est aussi celui qui peut les mobiliser pour ses objectifs stratégiques, n'est-ce pas l'Etat fédéral américain sous les administrations Truman et Eisenhower qui avaient mobilisé les entreprises pour construire les systèmes de défense face à l'URSS ? Le résultat de cette mobilisation des ressources fut désigné par l'expression de « complexe militaro industrielle ». La rupture technologique permanente du cyberespace conduit, à travers le recours au nationalisme pour la mobilisation des ressources humaines à l'émergence d'un nouveau complexe militaro informationnelle structurant pour les relations sino américaines.

LE CYBERNATIONALISME ET LE MERCENARIAT

Le large éventail des groupes sociaux mobilisables, cybersoldat, hacker, expert d'entreprise constitue la puissance numérique de la Chine. C'est l'allégeance au pays, la loyauté à un Etat qui est le levier de cette mobilisation sociale d'un acteur chinois du cyberespace par l'État. Ce levier est à la fois le résultat d'une éducation et d'une coercition sur les acteurs chinois du cyberespace. Celui qui est autonome en termes de loyauté devient rapidement un ennemi de l'intérieur, un dissident. L'Etat exerce un contrôle puissant sur la mobilisation des capacités de tous les types de cyberguerriers pour répondre à une situation donnée. Les cyberdissidents avec des capacités de cyberarmes significatives sont très peu nombreux. Ce levier de contrôle provient de la force du couplage entre le PCC et la gouvernance des entreprises chinoises du secteur numérique qui mettent en œuvre les compétences et le savoir-faire nécessaire autant que du développement des forces militaires dans le cyberespace. Au contraire, dans une démocratie libérale, un acteur du cyberespace, sous contrat avec une entreprise peut développer ses capacités et négocier sa loyauté, voire devenir un mercenaire au

service d'une puissance étrangère. Les acteurs non étatiques et leur loyauté à l'égard de leur Etat de référence sont de fait la clé de voûte des politiques de cybersécurité ce qui conduit à une articulation particulière entre État et entreprise dans ce secteur économique. ■

BIBLIOGRAPHIE

ASSOCIATED PRESS. (3/12/2016). Des experts américains tirent le signal d'alarme sur la cybersécurité,. *le Monde,*.

CABANES, B. (2013, oct-déc). Un drame à la mesure du monde. *L'Histoire*, p. n°161.

CABESTAN, J. P. (2005). Les multiples facettes du nationalisme chinois. *Perspectives chinoises n°88*, pp28-42.

CONRAD, P. (2015, printemps). Guerre industrielle, guerre totale. *La nouvelle revue d'histoire*, p. Hors série n°10.

DUBOIS, D., PRADE, H., & SMETS, P. (mai 1996). Representing partial ignorance. *IEEE Trans. on systems man & cybernetics, Vol 26 Issue: 3*, p 361 – 377.

FALIGOT, R. (2010). *Les services secrets chinois : De Mao à nos jours,.* Nouveau Monde Editions.

FERRERA, M. (2002). Intégration européenne et citoyenneté nationale et sociale, une analyse dans la perspective de Stein Rokkan. *Revue française de sociologie*, 277-306.

FOX-BREWSTER, T. (21/9/2016,). Watch chinese hackers control Tesla's brakes from 12 miles away. *Forbes,*.

FRIESER, K. (2003). *Le mythe de la guerre éclair.* Paris: Belin.

IHS. (2016, novembre 5). *Informatique : les "honkers" pirates chinois*. Récupéré sur Institut d'Histoire Sociale: http://est-et-ouest.fr/chronique/2015/151105.html

KISSINGER, H. (2014). *World order.* New York: Penguin Press.

LA TRIBUNE. (19 mai 2014). Cyberespionnage : la justice américaine inculpe des officiers chinois. *La Tribune*.

LA TRIBUNE. (22 avril 2014). Cyberespionnage, les Etats sont les plus grand pirates. *La Tribune*.

LE FIGARO. (2016, mars 11). *Les États-Unis s'apprêtent à lâcher leur contrôle des adresses Internet*. Récupéré sur Le Figaro: http://www.lefigaro.fr/secteur/high-tech/2016/03/11/32001-20160311ARTFIG00072-les-etats-unis-s-appretent-a-lacher-leur-controle-des-adresses-internet.php

LE PARISIEN. (27/10/2016,). Cyber attaque aux Etats-Unis : 100 000 objets connectés piratés. *Le Parisien,*.

MONTBRIAL, T., & KLEIN, J. (2000). *Dictionnaire de stratégie.* Paris: PUF.

RANOU, J. (2013). *Histoire de la dissuasion nucléaire.* -: -.

TRAN DAI, C. (février 2011). La Chine et l'Internet des choses : stratégie, opportunités et défis,. *Programme Chine 2.0, Centre Asia*.

TRUJILLO, E. (17/11/2016). Un logiciel espoin chinois découvert dans des milliers de smartphones Android. *Le Figaro*.

YAN, S., & JIANG, S. ((Juillet 2016),). US sentence chinese hacker for stealing military information,. *BBC*.

ASIA FOCUS #17

LE CYBERESPACE ET LE NATIONALISME CHINOIS : Le levier d'une grande puissance numérique

PAR EMMANUEL MENEUT

FÉVRIER 2017

Emmanuel MENEUT, ingénieur de l'école Centrale de Marseille (1990), diplômé de l'Université américaine de Paris (2008) et docteur de l'Institut Catholique de Paris (2012), est un politiste spécialiste de l'impact des ruptures technologiques sur les régimes de sécurité internationale en Asie. Intervenant extérieur en Master de relations internationales dans les universités catholiques, des écoles d'ingénieurs et de management, il est l'auteur de nombreux articles sur les enjeux de la géopolitique des dilemmes de sécurité.

ASIA FOCUS
Collection sous la direction de Barthélémy COURMONT, directeur de recherche à l'IRIS, maître de conférence à l'Université catholique de Lille, et Emmanuel LINCOT, Professeur à l'Institut Catholique de Paris – UR « Religion, culture et société » (EA 7403) et sinologue.
courmont@iris-france.org – emmanuel.lincot@gmail.com

PROGRAMME ASIE
Sous la direction de Barthélémy COURMONT, directeur de recherche à l'IRIS, maître de conférence à l'Université catholique de Lille
courmont@iris-france.org

INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES
2 bis rue Mercoeur
75011 PARIS / France

T. + 33 (0) 1 53 27 60 60
contact@iris-france.org
@InstitutIRIS

www.iris-france.org