RAPPORT FINAL

Composantes politico-militaire, économique et sociétale d'une cyberstratégie française : agir dans la dimension sémantique du cyberespace

FRANCOIS-BERNARD HUYGHE, Directeur de recherche
OLIVIER KEMPF, Chercheur associé
NICOLAS MAZZUCCHI, Chercheur associé

Juin 2014

IRIS - 2 BIS RUE MERCOEUR - 75011 PARIS - FRANCE
TÉL : +33 (0)1 53 27 60 60 - FAX : +33 (0)1 53 27 60 70 - WWW.IRIS-FRANCE.ORG

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

Introduction

Rares sont ceux qui doutent de la nécessité d'une cyberdéfense nationale. On peut discuter de son organisation, de l'ampleur des efforts entrepris, de son financement ou de son développement mais, au final que notre pays doive assurer son indépendance contre des dangers venus du cyberespace, voilà qui ne fait guère débat.

Aussi, cette étude ne porte-t-elle pas essentiellement sur les infrastructures numériques, la protection, la résilience et la cybersécurité en général, mais sur des enjeux stratégiques. Partant de l'analyse de cas pratiques de cyberagressions, elle se propose de discerner les logiques (technique, stratégique, parfois idéologique) qui se profilent derrière les attaques.

En cyberstratégie, l'incertitude ne naît pas seulement de la difficulté d'attribuer l'attaque, mais aussi des aléas qu'implique l'emploi d'armes nouvelles et souvent pas ou peu testées, notamment parce qu'elles sont souvent à emploi unique. L'incertitude est également liée à l'interprétation des faits et des intentions : avons-nous bien compris le « message » ? l'enchaînement des réactions est-il bien celui qui était espéré ?

L'incertitude est aussi à la mesure des possibilités stratégiques qu'ouvre le cyberespace. Ce dernier est hétérogène. D'ailleurs la majorité des chercheurs le décrit comme divisé en « couches ».

La couche matérielle est composée de tous les appareils et vecteurs comme les câbles, nécessaires à l'interconnexion générale. Les objets qui composent cette couche sont situées sur le territoire d'un État. Ils peuvent subir des opérations de pénétration, destruction, altération, contrôle ; une réalité à rappeler alors que le cyberespace est souvent décrit comme affranchi des contraintes matérielles ou des frontières.

La couche dite logique ou logicielle est celle des codes, algorithmes, programmes et standards qui permettent le fonctionnement des machines et l'interaction sur Internet. Ceux-ci représentent une force normative (*code is law*) ; ils structurent des informations. Partant, ils commandent indirectement des machines comme les systèmes SCADA et des personnes. Nombre des cyberagressions agissent sur le code informatique soit pour empêcher un système d'information de fonctionner, soit pour donner des ordres illicites. Cette prise de pouvoir change les règles de l'affrontement, valables dans les autres espaces de combat.

Le cyberespace comporte une troisième couche, dite sémantique, formée de tous les signes qui y circulent et qui ont du sens pour les acteurs. Ceux-ci tendent à agir en fonction de leurs représentations, susceptibles d'être altérées de manière délibérée. Nous donnons la priorité à cette couche, à la fois pour dépasser une analyse strictement technocentrée et parce que le but ultime de tout conflit est d'agir sur des cerveaux humains. Au-delà des résultats quantifiables (tant d'ordinateurs compromis, une panne qui dure tant et coûte tant), une cyberattaque vise forcément un effet de croyance et une volonté :

- croyance erronée de la victime quant à la situation et la réalité des forces ;
- conviction qu'il faut céder à la volonté de l'adversaire, ce qui est une victoire au sens clausewitzien le plus strict ;
- croyance négative ou positive en une cause ;
- choix de la réaction à adopter pour la fois suivante, donc prévisibilité de la conduite des acteurs.

Cette interaction entre choses, codes et personnes suscite une multitude de possibilités stratégiques. Selon une distinction communément admise, une cyberagression peut viser à dérober des connaissances précieuses, à paralyser, fausser ou détruire un système de commandement ou à produire un effet de tromperie, démoralisation, menace, etc.

Dans les trois cas – prédation, perturbation ou manifestation symbolique – il s'agit d'une violence qui, comme celle des armes classiques, a des effets en termes de capacité ou d'influence et sert des objectifs stratégiques. Les effets se manifestent à la fois dans le monde matériel et immatériel. Cela rend l'offensive tentante car elle semble anonyme, peu coûteuse et modulable.

En analysant des cas pratiques, nous avons dégagé des catégories, mais celles-ci peuvent se combiner : une attaque peut comporter de l'espionnage et du sabotage, viser la couche matérielle à travers la couche logicielle, être à la fois géopolitique et économique, associer divers acteurs, etc.

Le raisonnement stratégique ne peut se contenter de décrire cet arbre des possibilités. Toujours en partant des cas analysés, l'étude fait apparaitre les choix préférentiels des acteurs et les actions les plus probables ainsi que leurs enchainements parfois imprévus.

Reconstituant le trajet qui va de la conception à la mise en œuvre et aux conséquences, la première partie de l'étude se place du point de vue des acteurs. Elle décrit leur nature et leurs

interactions avec un environnement changeant ; il dépend des possibilités technologiques, des alliances, mais aussi de normes et de standards. Cette analyse doit aussi rendre justice à la part des représentations dans les décisions, notamment les cultures et les choix stratégiques faits en amont.

Une seconde partie s'intéresse à l'action elle-même. Une fois prise la décision stratégique, les acteurs font des choix pratiques. Leurs résultats dépendent de cette part de brouillard et de friction qui s'interpose entre le dessein et sa réalisation, mais ils reflètent aussi l'efficacité des discours et les effets des techniques de contrainte et d'influence.

Toutes les potentialités de la technologie ne sont pas forcément mises en œuvre ; des facteurs tenant aux représentations des acteurs restreignent à la fois le nombre de « coups » qui peuvent se jouer, le niveau d'escalade et l'ampleur des ravages.

Partie I : L'intention des acteurs

Cette première partie traitera successivement de l'intention des acteurs (chapitres 1 et 2), de la façon dont ils peuvent affecter l'environnement (chapitres 3 et 4) et enfin des raisons des choix qu'ils opèrent (chapitres 5 et 6).

Chapitre 1 - Typologie des acteurs

La stratégie est, selon le général Beaufre, « la dialectique des volontés employant la force pour résoudre leur conflit ». Or, qui dit volonté dit sujet individuel ou collectif. Trois catégories seront mobilisées : les États, les organisations et les individus.

I Etats et organisations publiques

Traditionnellement, la stratégie est une affaire de souveraineté. Même si la théorie des Relations Internationales a pris acte de l'émergence de nouveaux acteurs, la place des Etats reste centrale même dans le cyberespace.

11 Etats

Il est rare que deux États utilisent le cyberespace dans le cas d'un conflit déclaré. Le cas Georbot, dans la guerre entre la Géorgie et la Russie en 2008, est quasiment le seul exemple.

Ce conflit à une suite dans le cyberespace : en 2011, le Computer Emergency Response Team (CERT)[1] géorgien découvre un maliciel sur 400 ordinateurs de six administrations, les machines formaient un *botnet*[2]. Ce réseau aurait été controlé par un certain Artur Jafuniaev, au nom de la société WSDomains, domiciliée au 13, rue Lubianka, 346713, Moscou ; cette adresse est celle du ministère russe de l'Intérieur.

Même dans un cas comme celui-là, il n'y a pas de preuve absolue de la culpabilité des autorités russes. En revanche, il est rare de voir un cas où des autorités étatiques rendent publiques une tentative d'agression par un autre Etat.

Mais que signifie « l'Etat » dans ce contexte ? Ainsi, dans l'affaire dite Dark Seoul en 2013, des sites gouvernementaux et des ordinateurs de trois banques nationales et trois chaînes de télévision de Corée du Sud furent la cible de maliciels qui mirent hors d'usage 48 000 ordinateurs. Symantec évoquait des agressions contre la Corée du Sud[3] et le New York Times

[1] Equivalent d'un centre de crise pour le cyberespace.
[2] Réseau d'ordinateurs ou robot fantômes communiquant ensemble.
[3] Symantec, "Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War", http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war, 26 juin 2013.

titrait en avril : « *South Korea Blames North for June Cyberattacks*[4] ». Pourtant, la Corée du Sud refusant de désigner un coupable et la Corée du Nord démentant toute implication, rien n'est officiel.

111 Organisation ad hoc de l'exécutif

La plupart des États ont mis en place des unités spécialisées de cyberdéfense. L'organisation minimale repose sur des équipes d'urgence et de réaction aux incidents informatiques comme les CERT. Les États les plus développés peuvent avoir des dispositifs plus spécialisés, voire très volumineux liés le plus souvent à l'organisation militaire ou aux services de renseignement. Ainsi, la National Security Agency (NSA) compterait 35 000 employés directs et jusqu'à 60 000 en incluant les différents services cyber des Armées dont le Cybercommand[5].

Au Royaume-Uni, le Government Communications Headquarters (GCHQ) est le service de renseignement cyber sous tutelle du ministère des Affaires Etrangères. En Allemagne, l'Office fédéral de la Sécurité des technologies de l'Information (Bundesamt für Sicherheit in der Informationstechnik ou BSI) tient une fonction en partie comparable et dépend du ministère de l'Intérieur. En France, l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) est placée sous l'autorité du Secrétaire Général de la Défense et de la Sécurité Nationale (SGDSN), qui dépend du Premier ministre. Un Officier général Cyberdéfense est en charge de ces sujets à l'état-major des armées du ministère de la Défense. En Estonie, l'Autorité des Systèmes d'Information (Estonian Information System's Authority ou RIA) avec son bras armé, le département de protection des infrastructures critiques (Department of Critical Information Infrastructure Protection ou PIIC) est rattachée au ministère des Affaires economiques et des communications. Ces quatre exemples européens montrent que les autorités de tutelle varient selon les priorités nationales : Affaires étrangères, Défense, Intérieur, Économie.

Des pays donnent des compétences à certains de leurs services de renseignement. En Israël, les actions particulières sont conduites par l'unité 8200 dépendant de l'armée israélienne[6]. Pour la Chine, le rapport Mandiant publié aux Etats-Unis en 2013 désigne l'unité 61398

[4] http://www.nytimes.com/2013/07/17/world/asia/south-korea-blames-north-for-june-cyberattacks.html?_r=0
[5] De plus, la NSA emploie des *contractors* (sous-traitants).
[6] Voir Olivier Danino, « La stratégie cybernétique de l'Etat d'Israël », *Sécurité Globale,* n° 2013/2, pp.15-24.

dépendant du 3ème département du 2ème bureau de l'armée, comme le principal organisme offensif chinois.

112 Législatif

Aux Etats-Unis, le *Patriot Act* (section 215) voté par le Congrès couvre une grande partie de l'activité cyber de la NSA, comme cela a été dévoilé lors de l'affaire PRISM[7]. Une législation de 2008 a étendu ces capacités via la loi FISA[8]. S'y ajoutent plusieurs directives présidentielles. L'origine du droit cyber est donc à la fois législative et exécutive.

Une distinction similaire se retrouve en France puisque la Loi de programmation militaire (LPM) de 2013 prévoit plusieurs dispositions cyber[9]. L'ANSSI fut créée par décret en application : « *Le décret n° 2009-834 du 7 juillet 2009 créant l'Agence nationale de la sécurité des systèmes d'information donne à cette agence, en plus de la sécurité des systèmes d'informations de l'État, une mission de conseil et de soutien aux administrations et aux opérateurs d'importance vitale, ainsi que celle de contribuer à la sécurité de la société de l'information, notamment en participant à la recherche et au développement des technologies de sécurité et à leur promotion*[10] ».

113 Judiciaire

La loi FISA de 2008 a établi un tribunal spécial pour contrôler la NSA : la Foreign Intelligence Surveillance Court (FISC) dont l'action a été controversée. Elle aurait accepté plus de 99 % des demandes d'autorisation de surveillance qui lui ont été transmises, tandis que son fonctionnement est particulièrement opaque.

Outre les cours spéciales, les juridictions ordinaires peuvent se prononcer. Ainsi, à dix jours d'écart, deux avis contradictoires ont été rendus par des juges américains. Le 17 décembre 2013, au tribunal du District de Columbia, le juge Richard J. Leon a estimé en première instance que les écoutes de la NSA violaient le 4e amendement de la constitution qui interdit

[7] Par convention, nous appellerons « affaire PRISM » l'ensemble des faits révélés par E. Snowden.
[8] « En 2008, le Congrès a autorisé une version de ce programme qui permet à la NSA d'accéder sans mandat à tout *« renseignement étranger »*, soit toute communication entre des ressortissants américains et des « cibles » étrangères suspectes. La disposition juridique correspondante est la Section 702 du *Foreign Intelligence Surveillance Act* (la loi sur la surveillance et le renseignement étranger). » *Le Monde*, 27 octobre 2013, http://abonnes.lemonde.fr/technologies/article/2013/10/27/espionnage-de-la-nsa-quels-recours-juridiques-pour-les-citoyens-francais_3503775_651865.html La distinction entre « étrangers » qui peuvent être surveillés et citoyens américains dont les messages et métadonnées ne peuvent être consultés sans un mandat légal (*due warrant*) fonde ainsi toute la logique du système. Logique toute théorique au regard des réalités du numérique.
[9] Gal Watin-Augouard, « La LPM et la cybermenace », *Observatoire du FIC*, 22 octobre 2013, http://www.observatoire-fic.com/la-lpm-et-la-cybermenace-par-le-general-darmee-2s-marc-watin-augouard/
[10] Site de l'ANSSI : http://www.ssi.gouv.fr/fr/anssi/presentation/l-historique-de-l-anssi.html

les perquisitions injustifiées chez les citoyens. Dix jours plus tard, un autre juge de New York estimait quant à lui que ces écoutes étaient légales et que le programme de riposte au terrorisme justifiait ces pratiques. La Cour suprême aura à trancher.

12 Organisations internationales

Les organisations internationales publiques ont les États pour parties prenantes. Elles peuvent être des acteurs actifs (prenant des initiatives), ou passifs (comme cible des actions des autres).

La plupart des organisations internationales sont permanentes. Ainsi de l'Organisation des Nations-unies (ONU), de l'Union européenne (UE), de l'Organisation mondiale du commerce (OMC) ou du Comité international olympique (CIO). La plupart de ces organisations ont été victimes de cyberagressions, toutes ou presque ont été espionnées. Ainsi, l'ONU par les Etats-Unis mais aussi par la Chine. Lors de l'affaire Aurora en 2010, imputée à la Chine, 65 organisations internationales auraient été surveillées dont le CIO. Les organisations internationales peuvent adopter des mesures de protection (par exemple, l'Alliance atlantique a développé une politique active de cyberdéfense à la suite de l'agression contre l'Estonie en 2007[11]), ou élaborer des stratégies plus complètes (l'Union européenne a rendu publique en février 2013 sa stratégie de cybersécurité).

Certaines organisations peuvent être de circonstance. Ainsi la Force internationale d'assistance et de sécurité (FIAS), à l'origine (2001) établie entre États sous un mandat de l'ONU est passée sous le contrôle de l'Organisation du Traité de l'Atlantique Nord (OTAN) en 2003. Elle a mené quelques actions cyber, par exemple durant la « guerre des tweets », en 2011, contre les Talibans[12]. En plusieurs occasions, les réseaux sociaux ont joué le rôle d'un champ de bataille où se sont opposés la FIAS et les groupes armés.

Certains acteurs exercent une mission publique de niveau quasi interétatique. Ainsi, l'Internet Corporation for Assigned Names and Numbers (ICANN) est une société de droit californien, sous la tutelle du ministère américain du Commerce et a le monopole de la gestion et de

[11] Voir O. Kempf, « L'Otan et la cyberdéfense », Chaire cyberdéfense Saint-Cyr, http://www.st-cyr.terre.defense.gouv.fr, mai 2013.

[12] Si des moyens cyber de la couche logicielle ont été utilisés en Afghanistan, peu de détails ont filtré. On apprit ainsi, à propos du décès étrange d'un espion britannique en 2010, Gareth Williams, que celui-ci servait au GCHQ et avait « cassé les codes cryptologiques des talibans ».

l'attribution des plages d'adresses IP et indirectement des noms de domaine[13]. Mais cette tâche pourrait être également remplie par l'Union internationale des télécommunications (UIT) qui appartient au système onusien. Lors du sommet de Dubaï de l'UIT, tenu en décembre 2012, les États membres ont refusé de lui octroyer un pouvoir étendu, malgré les enjeux politiques. [14]. Le gouvernement américain a annoncé le 14 mars 2014 son intention de réviser le contrôle de fait qu'il exerce sur les noms de domaine[15]. Par ailleurs « *le pouvoir réside dans les droits d'écriture dans la racine unique qui est au sommet de l'arborescence. Si théoriquement il revient à l'ICANN de faire évoluer son contenu, selon le contrat IANA (Internet Assigned Numbers Authority) attribué par le Department of Commerce (DoC), l'opérateur technique est la société américaine Verisign (qui gère par ailleurs l'extension .com), également sous contrôle du DoC*[16] *»*. Des organismes qui sont en droit des sociétés commerciales ou des organisations privées, assurent de fait des fonctions de service public international.

13 Quasi États

Certaines organisations ne sont pas, *de jure*, des États. Outre l'Autorité palestinienne, on peut mentionner la structure organisée autour du Dalaï Lama et du gouvernement tibétain en exil. Cette organisation politique est surtout vue par les autorités de Pékin comme un danger. Ainsi, l'affaire Ghostnet a été une très importante manœuvre d'intrusion dans les réseaux tibétains, très probablement par les Chinois.

Les ordinateurs de l'Office du Lama à Dharamsala, d'ONG tibétaines en Inde et des missions de New York, Londres et Bruxelles ont été frappés par un maliciel nommé Ghostnet. Certains ordinateurs de contrôle auraient été localisés en Chine (Hainan, Sichuan, Guangdong et Jiangsu). Un État aurait espionné une organisation para-étatique. La révélation de Ghostnet en 2009 n'a pas mis fin à cette activité ; l'affaire Luckycat, révélée en 2012, a montré que les réseaux indépendantistes tibétains continuaient d'être espionnés.

[13] Notamment les noms de domaine en .com puisque l'ICANN contre Verisign, l'organisme responsable de l'attribution de ces derniers.
14 Voir N. Mazzucchi, « La conférence de Dubaï : la régulation du net n'aura pas lieu », *Sécurité Globale* n° 2013/2, pp.41-47 ; voir infra.
[15] Voir par exemple le commentaire de l'AFNIC : http://afnic.fr en date du 12 mai 2014
[16] D. Lacroix, « Ranger la planète, Le nommage des domaines est-il l'expression d'une stratégie américaine de domination des réseaux ? » in « O. Kempf (dir), *Penser les réseaux*, L'Harmattan, Paris, 2014 (à paraître).

II Organisations

Dans la société internationale d'autres acteurs que les gouvernements ont émergé, surtout dans la décennie après de la Guerre froide[17] : les firmes multinationales, les médias et les autres organisations non-gouvernementales (ONG).

21 Sociétés commerciales du cyberespace

Le cyber est d'abord un objet technique et concret, reposant sur des machines reliées, ce qui suppose des fabricants. Chacun incorpore plus ou moins de fonctions de sécurité et constitue un actif stratégique potentiel, surtout si le savoir-faire est rare. La dépendance à l'égard d'un acteur particulier pose des questions stratégiques. C'est pourquoi le sénateur Bockel dans son rapport sur la cyberdéfense s'inquiète des routeurs de cœur de réseau, l'action des constructeurs chinois soulève un problème de souveraineté. De même, la ministre déléguée à l'Economie numérique déclare que l'activité de pose de câbles sous-marins assurée par Alcatel est stratégique.

Ces machines ont besoin de logiciels et de protocoles de réseau. Certains ont longtemps suspecté que le système d'exploitation Windows comportait des « portes dérobées » qui permettaient d'observer les usages des utilisateurs. Le Canard enchaîné au début des années 2000 a critiqué la passation d'un contrat entre le ministère de la Défense et Microsoft qui n'aurait pas donné toutes les garanties de sécurité. Les Russes développeraient un système d'exploitation fondé sur une technologie en source ouverte, afin de ne plus dépendre de Windows. Un ministre français a également évoqué ce sujet au printemps 2014. De même l'Etat chinois a banni en 2014 le système Windows 8 de ses administrations. Les sociétés de télécommunications sont également des acteurs importants. Ainsi, le scandale PRISM a commencé par l'affaire Verizon en juin 2013.

Des sociétés de service spécialisées dans la cybersécurité comme les sociétés d'antivirus ont souvent découverts les principaux maliciels de ces dernières années. Stuxnet, Gauss ou Flame ont tous été découverts par des sociétés russes ou d'Europe de l'Est et la plupart des cas attribués à la Chine (Aurora, Titan Rain) par des sociétés américaines. En dehors de toute

[17] Voir Charles-Philippe David, *La guerre et la paix*, 3ème édition, Presses de Sciences Po, 2013.

différence technique, les clients tendent à se tourner vers certaines société d'une nationalité donnée parce qu'elles leur semblent offrir plus de garanties.

Le cyberespace a permis le développement d'une économie spécialisée offrant des produits d'usage et de socialisation tels les réseaux sociaux et qui exploitent des quantités énormes de données et metadonnées (*Big data*). Or, ces sociétés dont le GAFA pour Google, Apple, Facebook et Amazon, ont une valeur stratégique et sont toutes soupçonnées d'avoir collaboré avec les autorités américaines dans le cadre du programme PRISM. De même, la Chine a développé une stratégie d'indépendance afin que ses grands acteurs soient nationaux : Alibaba, Tencent, Baidu et Weibo ont un monopole de fait sur la clientèle chinoise, ce qui permet aux autorités de mieux contrôler leur propre population, de se protéger de la cybersurveillance étrangère et de générer du profit national[18].

22 Autres sociétés

Toutes les sociétés ont désormais une présence dans le cyberespace. Toutes les entreprises manient de l'information plus ou moins sensible. On ne compte plus les affaires d'espionnage économique utilisant les outils cyber. Nombre de cas étudiés touchent à des sociétés stratégiques : entreprises du secteur de la défense ou de haute technologie (affaire Aurora), mais aussi du secteur de l'énergie (nucléaire en particulier, comme l'affaire Areva). Toutefois, toutes les entreprises peuvent être touchées, dont des banques (affaires Dark Seoul, Gauss, Itsoknoproblembro).

Cet espionnage peut avoir des conséquences dramatiques pour l'entreprise comme pour Nortel qui aurait été espionnée pendant dix ans, perdant des brevets et subissant une perte d'image aussi bien qu'une perte économique.

23 Groupes criminels

Certaines organisations criminelles employant des spécialistes informatiques de haut niveau peuvent être classées parmi les acteurs stratégiques, même si leur but ne l'est que marginalement. La cybercriminalité organisée touche plus à la cybersécurité qu'à la

[18] Voir Vivien Fortat et Olivier Kempf, « Cyberstratégie chinoise : du contrôle à l'expansion », *AGIR, revue de la société de stratégie*, octobre 2013.

cyberdéfense, mais ces mafias peuvent être instrumentalisées par des États qui souhaitent ne pas apparaitre directement ou servir de sous-traitants par des organisations terroristes. Il est très probable que les mafieux russes du Russian Business Network ont participé à l'agression contre l'Estonie. Toutefois, il n'est pas facile de savoir quelle barrière sépare l'exécutant du donneur d'ordre. Des opérations peuvent poursuivre plusieurs buts : obtenir à la fois des renseignements directement monnayables et d'autres qui ne sont importants qu'aux yeux d'un commanditaire politique.

24 Groupes armés

Les groupes armés sont des acteurs stratégiques de nature diverse et différemment organisés. Ainsi, les Shebabs somaliens sont un groupe armé ayant des objectifs politiques qui ont pu un moment contrôler de vastes régions du territoire somalien. Leurs moyens de communication semblent rustiques néanmoins ils sont très actifs sur les réseaux sociaux. Ils se servent particulièrement de Twitter à des fins d'agit-prop[19]. Comme la plupart des groupes terroristes, ils s'en servent pour donner un maximum de publicité à leurs actions, notamment auprès des médias internationaux, provoquer symboliquement l'adversaire et rallier des partisans. De même, les Talibans paraissent beaucoup plus organisés. La « guerre des tweets » montre comment la FIAS d'un côté et les Talibans de l'autre se sont opposés sur le théâtre d'opération des réseaux sociaux.

Al Qaida est un groupe terroriste non centralisé, pour ne pas dire une « marque franchisée ». Ainsi, des groupes jihadistes d'initiative locale ou poursuivant des objectifs territoriaux plus immédiats que l'établissement du califat universel, se rattachent à Al Qaida ne serait-ce que de manière formelle. Ils n'utilisent pas le cyberespace pour des sabotages de grande ampleur, contrairement à un fantasme régulièrement évoqué, mais soit pour communiquer, soit surtout pour organiser une propagande sans frontières[20]. Cela leur permet de s'affranchir de leur base géographique et de s'adresser à des individus dispersés partout dans le monde[21].

[19] Voir infra.
[20] Ou, ce qui revient au même, pour laisser s'auto-organiser des forums, groupes de discussion et autres réseaux plus ou moins spontanés. Les néophytes peuvent y exprimer leur désir de vengeance pour les injustices subies par les musulmans, voire leur volonté de rejoindre le jihad via un processus communautaire d'expression de la colère et de recrutement.
[21] Voir O. Kempf, « Le cyberterrorisme : un discours plus qu'une réalité » in *Hérodote*, printemps 2014.

25 Groupes politiques

Les groupes politiques peuvent utiliser le cyberespace dans une perspective stratégique sans employer directement les armes. Ainsi, le Hezbollah a une activité multiforme dans le cyberespace. Les réseaux sociaux lui ont servi à des manœuvres d'espionnage contre Israël, soit en exploitant des fautes individuelles[22], soit à travers des pièges sociaux[23]. L'utilisation de la couche sémantique sert également à la subversion, comme l'a montré la campagne médiatique sur les réseaux sociaux au cours de la guerre de 2006[24].

D'autres groupes politiques peuvent agir différemment. L'affrontement « amateur » entre la « cyberarmée pakistanaise » et la « cyberarmée indienne » consista en des campagnes de DDOS[25] et autres défacements de sites n'ayant guère touché le grand public. L'Armée électronique syrienne (AES)[26] qui a démontré de véritables capacités de piégeage électronique comme celui du compte de l'Associated Press, et choisi des cibles à haute valeur médiatique : là encore, l'essentiel se déroule dans la couche sémantique. Dernier exemple, le groupe Epée Tranchante de la Justice qui a revendiqué l'agression Shamoon. Ce groupe activiste se revendique d'une vague idéologie islamiste. Il semble surtout chercher dans le cyberespace d'autres moyens de faire valoir son discours (couche sémantique) grâce à l'efficacité du virus (couche logique)[27].

26 Autres acteurs

La presse peut être une cible comme l'illustre l'exemple de l'Associated Press : la notoriété de la cible a maximisé la portée de l'opération ; l'opinion a retenu qu'un groupuscule syrien proche du régime pouvait pirater un grand nom comme AP.

[22] Un conscrit qui annonce la veille sur Facebook la date et le lieu d'une opération qui doit être annulée en catastrophe.
[23] Ainsi, sur Facebook, l'accorte amie de nombreux membres des forces spéciales israéliennes, et qui dissimulait un observateur chiite libanais
[24] Voir Balthazar Dax, « Le flou de la victoire du Hezbollah en 2006 », *Revue Défense Nationale*, janvier 2014. Sur la notion de flou de la victoire, voir G. Blum, « Fog of victory », *European Journal of International Law*, 2013/24, pp. 399-421.
[25] Le Déni de Service Distribué est une attaque cherchant à mettre hors-service des serveurs par un nombre très important de requêtes automatiques.
[26] Pour être objectifs, il faut préciser que les membres de l'AES sont présentés par certains comme des spécialistes de haut niveau forcément liés à des services spéciaux syriens, par d'autres comme des amateurs menant des attaques d'une grande banalité et incapables de défendre leurs propres comptes sur Dropbox.
[27] Les liens entre Epée tranchante de la justice et l'Etat iranien n'ont jamais ni prouvés, ni démentis.

La presse peut surtout être un amplificateur formidable et accréditer certaines informations. Ainsi, les documents diffusés par Wikileaks dans l'affaire dite du cablegate prennent une toute autre ampleur le jour où des grands organes de presse européens publient des extraits et des analyses des documents.

Dans l'affaire PRISM, E. Snowden a réussi à toucher le grand public au travers de médias traditionnels : initialement le Guardian, puis le New York Times, Der Spiegel, Globo, Le Monde.

Les laboratoires d'idées (think-tanks) et groupes d'experts jouent également un rôle en cyberstratégie. C'est le cas de la Rand Corporation, dont certaines publications ont très tôt posé les bases de la réflexion stratégique dans le cyberespace. En France, outre les think tanks traitant habituellement des questions de sécurité et de défense, deux institutions soutenues par des entreprises se consacrent exclusivement à cet espace comme la chaire Castex de cyberstratégie ou la chaire de cyberdéfense et cybersécurité de Saint-Cyr.

Les acteurs économiques prennent également leur part. Ainsi la société américaine Mandiant dont le rapport sur le cyberespionnage chinois a eu un grand impact, ou la société française CEIS qui co-organise le Forum International de Cybersécurité se présente comme un acteur majeur de la cyberstratégie française. Il ne s'agit pas simplement d'influence, mais aussi de normalisation.

III Acteurs individuels

Une des nouveautés du cyberespace tient à l'émergence de l'individu comme acteur stratégique. La technique donne à chacun du pouvoir (de s'exprimer, de s'informer, de se coordonner avec la communauté de son choix, de lutter)[28] mais elle lui permet aussi de se former sa propre bulle informationnelle à l'abri des messages diffusés par les médias de masse[29] .

[28] C'est ce que les anglo-saxons désignent sous le nom *d'empowerment* des individus ; voir C. Shirky, *Here Comes Everybody : The Power of Organizing Without Organizations,* Londres, Penguin, 2008.
[29] Ce qui ne veut pas dire en étant plus critique ou moins naïf pour autant ; voir G. Bronner, *La démocratie des crédules,* Paris, PUF, 2013

31 Militants

Les Anonymous sont apparus entre 2003 et 2006 et sont considérés tantôt comme un groupuscule de quelques hackers, tantôt comme un mouvement citoyen international. Il s'agit d'un réseau totalement décentralisé et sans organisation, ni chef où la prise de décision s'effectue autour d'un projet très général consistant à défendre la « citoyenneté du Net » sans manifeste ni doctrine. Le recrutement est des plus simples : il suffit de se déclarer membre d'Anonymous pour l'être. Cette facilité d'adhésion est à l'avantage des entrants comme des membres qui n'ont pas à s'astreindre à des tâches de recrutement. Ces actions sont simples[30] et ludiques ce qui les rend populaires, notamment auprès des jeunes générations connectées[31]. L'égalité de tous permet une prise d'initiative très décentralisée.

Les Anonymous ont su très tôt manier des symboles qui les ont rendus populaires. Désormais, il n'est plus un mouvement revendicatif où des manifestants n'arborent le masque de Guy Fawkes, mis en vogue par les Anonymous. Si le mouvement est d'origine nord-américaine, il apparaît comme typiquement occidental tant dans ses idéaux que dans sa composition.

Il n'existe pratiquement plus de mouvement de contestation, y compris physique, qui n'utilise le cyberespace pour mobiliser : Occupy Wall Street américain, Indignados espagnols, printemps érable québécois, Manif pour tous ou Bonnets rouges français, autant de mobilisations massives facilitées par le cyberespace. Les individus n'ont plus besoin de structures classiques d'intermédiation (associations, Eglises, syndicats, clubs, partis politiques) pour porter une parole collective, politique ou autre.

Les révoltes arabes de l'année 2011 ont constitué un exemple de cette mobilisation. Ce fut tout particulièrement le cas en Egypte où les manifestants étaient mobilisés par les réseaux sociaux, en synergie avec l'influence d'Al Jazeera. Sans tomber dans le mythe de la toute-puissance libératrice du Net dans les « révolutions 2.0 »[32], il faut noter que les réseaux sociaux ont permis la circulation de messages interdits par le pouvoir, ont poussé des individus à se mobiliser « dans la vraie vie », ont propagé les images et les idées des révoltes

[30] Les outils nécessaires à mener certaines opérations peuvent être trouvés sur Internet et mis en œuvre même par quelqu'un n'ayant pas un haut niveau de connaissances techniques.
[31] Voire Paul Jorion, *La guerre civile numérique,* Textuel 2011
[32] Titre d'un ouvrage (Steinkis, 2012) de Whael Ghonim, responsable local de Google, dont la page Facebook dédiée au blogueur Khaled Saïd (arrêté par la police) a contribué à propager les révoltes en Égypte.

dans les diasporas arabes et auprès des médias étrangers, et enfin ont servi à organiser les foules dans la rue[33].

Le régime égyptien tenta un moment de couper les liaisons Internet. En réponse, un certain nombre d'ONG occidentales, soutenues par l'administration américaine, réussirent à faire passer le matériel de transmission par satellite ou répandirent des méthodes de substitution pour permettre aux internautes égyptiens de poursuivre l'activisme en ligne. Le succès de cette guerre de l'information s'explique aussi par bien d'autres causes que la technologie ; les réseaux sociaux ont été les accélérateurs ou les amplificateurs des révoltes, non leur cause ni la garantie de leur succès.

Dans le cas syrien, Internet a entretenu la contestation, mais le régime a su riposter. Ainsi, lors de l'arrestation des opposants, les policiers ont très vite demandé les *login* et mots de passe pour infiltrer et perturber les réseaux contestataires, très vite également est apparue l'Armée électronique syrienne. Face aux « technologies de libération » ou si l'on préfère de contournement, apparaissent des technologies de contrôle[34], propagande et désinformation des gouvernements et de la « courbe d'apprentissage des dictateurs[35] » en matière numérique s'élève.

32 Lanceurs d'alerte (*Whistleblowers*)

Les lanceurs d'alerte sont apparus au XX^{e} siècle[36]. Ainsi, Daniel Ellsberg fournit au New York Times les documents sur la guerre du Viêtnam, qui furent connus sous le nom de *Pentagon papers*[37]. « Gorge Profonde » permit au Washington Post de révéler le scandale du

[33] Pour une analyse plus détaillée, voir « Les effets géostratégiques d'Internet : vers la création d'un territoire d'expression sans frontière », *étude EPS 2011-72* pour la DICoD, F.B. Huyghe directeur, K. Bitar, N. Arpagian, M. Pinard.

[34] Voir Observatoire géostratégique de l'information (Iris) « Technologies de libération vs contrôle technologique » : http://www.iris-france.org/docs/kfm_docs/docs/observatoire-geo-info/technologies-de-liberation-vs-contrle-technologique---iris---mai-2012.pdf

[35] Expression empruntée à W.G. Dobson, *The Dictator's Learning Curve*, New York, Anchor Books, 2012

[36] L'expression « *whistleblower* », renvoyant à l'idée d'un citoyen sifflant une faute commise par une organisation et qu'il est convenu de traduire par lanceur d'alerte, apparaît avec les pamphlets de Ralph Nader à cette époque. Voir « Cyberespace : le temps de l'après Snowden », *Observatoire géostratégique de l'information*, 10/03/2014 et Florence Hartmann, *Lanceurs d'alerte : les mauvaises consciences de nos démocraties,* Ed. Don Quichotte, 2014

[37] Ce qui l'obligea à photocopier clandestinement plusieurs milliers de pages.

Watergate. Il s'agissait à chaque fois de rendre publique une vérité secrète : un mensonge, une activité inavouable d'une importante organisation, passée ou actuelle.

Cet idéal inspire J. Assange, le fondateur du site Wikileaks[38], partisan d'une transparence absolue et lanceur d'alerte de profession. Wikileaks ne peut se concevoir que dans le cyberespace. Une fois abolies les difficultés techniques de la copie, de l'exfiltration et de la transmission, Wikileaks peut révéler d'énormes masses de documents classifiés. Edward Snowden, travaillant pour la NSA et motivé par une indignation morale a recueilli en quelques mois des documents internes puis il les a publiés à partir de l'été 2013 révélant ainsi les rapports complexes du secret d'État et des dispositifs techniques de surveillance[39]. Il a trouvé des relais remarquablement efficaces comme Glenn Greenwald[40] ainsi que dans de nombreux organes de presse qui ont contribué à entretenir « l'affaire Snowden ». Dans le cas de PRISM, une campagne de presse continue à produire des scoops. Un lanceur d'alerte n'est rien sans caisse de résonance et sans gestion du scandale dans le temps. De la même façon, Bradley Manning, soldat américain à l'origine du fameux *cablegate*, a transmis ses informations à Wikileaks qui les a rendues publiques.

33 Hackers

Le statut des hackers, ces individus auxquelles les compétences informatiques permettent de pénétrer des réseaux informatiques, varie considérablement. Ainsi la distinction entre hackers blancs et hackers noirs (parfois appelés crackers) repose sur leurs intentions. Certains sont utilisés par des États, sociétés ou mafias. Il existe aussi des regroupements de hackers ayant des objectifs politiques (hacktivistes). Il faut se garder de l'illusion du « bidouilleur de génie » qui réussit, dans son garage, à pirater les ordinateurs de la CIA : cela paraît peu probable de nos jours, à cause des multiples efforts de cyberprotection des installations de tout genre. Contre une cible bien défendue, un hacker isolé ne peut généralement pas grand-chose. Néanmoins, sans utiliser de méthodes très sophistiquées, un simple individu peut provoquer de vrais dégâts. Dans l'affaire Diginotar, un certain Comodohacker a piraté le certificat de sécurité qu'accordait l'autorité néerlandaise de certification des échanges électroniques. Six

[38] Si Wikileaks doit être rangé dans la catégorie des acteurs politiques, les catégories ne sont pas rigoureusement étanches. Il est mentionné ici parce que sa méthode relève du même système que les lanceurs d'alerte : divulguer des informations qui auraient du rester confidentielles.
[39] Voir Médium n° 37, « *Secrets à l'ère numérique »,* Octobre 2013.
[40] Ce journaliste, avocat et blogueur contacté anonymement par Snowden a été son véritable impressario. Il raconte cette aventure dans *Nulle part où se cacher*, J.-C. Lattès, 2014.

semaines plus tard, la société faisait faillite. Outre les conséquences d'un acte isolé, il faut signaler que cette agression cyber a eu des effets importants moins par le sabotage du système que par la perte de confiance qui en a résulté. Ceci nous ramène à la couche sémantique : les flux Internet reposent sur une confiance qui peut être compromise par un seul individu.

Chapitre 2 - Spécialisation sectorielle

Au-delà de l'identité des agresseurs et de leurs buts réels, supposés, révélés ou affichés, les cyberagressions se déroulent dans trois domaines d'action stratégique. Loin de s'en tenir à un cloisonnement strict entre les domaines géopolitique, militaire et économique, ces agressions témoignent de plus en plus d'une transversalité, qui peut leur être propre ou résulter des conséquences de l'action.

I Les trois domaines stratégiques

La conflictualité dans le cyberespace se déploie dans un espace géographique original régi par des règles propres. Trois domaines y constituent des champs d'affrontement à part entière avec leurs particularités. Le premier est militaire puisque la cyberstratégie peut être entendue comme l'approche d'une nouvelle sphère de déploiement et de manoeuvre de la force armée. La seconde est géopolitique, les cyberagressions visent les États et inaugurent une forme inédite de lutte pour la puissance entre acteurs des relations internationales. Enfin, le domaine économique, le plus récent des trois à être touché par la cyberconflictualité, en raison, entre autre, de la mondialisation des marchés et des facteurs de production.

11 Is Cyberwar coming ?

La conflictualité dans le cyberespace peut être militaire. En ce sens elle est l'extension cyber des actions cinétiques survenant lors d'un affrontement, à défaut, du moins pour le moment, de véritable « cyberguerre » telle que prophétisée dans les années 1990. Même si les déterminants et les spécificités du cyberespace diffèrent[41] de ceux des autres sphères stratégiques (terre, mer, air), il est néanmoins une sphère stratégique militaire, susceptible, comme le montrent depuis plusieurs années des études dédiées, de servir de « champ de bataille ».

Il peut s'agir d'un appui particulier aux opérations physiques traditionnelles. Il n'y a pas aujourd'hui de cyberguerre au sens classique car il y manque le taux de mortalité collective, l'implication ostensible et systématique d'acteurs souverains, la possibilité de terminer la guerre par une paix reconnue par l'Histoire, la territorialité des opérations, la désignation

[41] Notamment par le simple fait que le cyberespace est le seul espace stratégique qui ait été créé par l'homme.

officielle de l'ennemi et de la revendication soutenue par les armes comme caractéristiques des guerres. Cela a, jusqu'à présent, empêché le cyberespace d'être un espace de conflit *per se* mais non un appui transversal aux opérations classiques ou un lieu de détournement conflictuel. Suivant le Department of Defense américain, le niveau ultime de cybermenace – dit niveau VI – est représenté par les actions militaires combinées, utilisant le cyberespace en tant qu'élément d'une agression plus large[42] mobilisant des moyens physiques classiques contre les intérêts vitaux d'un pays. En l'état, seuls les Israéliens (Opération verger contre la Syrie en 2007) et les Russes (guerre contre la Géorgie en 2008) ont mis en œuvre de telles opérations. Le cyberespace peut aussi, dans le cadre d'une conflictualité militaire, servir comme élément de propagande ou d'opérations psychologiques, agissant sur le moral des adversaires.

La dimension sémantique de la cyberstratégie militaire, souvent éludée dans les études, est *de facto* prépondérante. L'interconnexion potentielle entre toutes les machines et la quasi-impossibilité de créer un système « étanche » dans le cyberespace en font un médium poreux par essence. Lorsque les dictatures du Maghreb et du Proche-Orient ont tenté de contrôler l'accès de leurs populations à l'information au moment des révoltes arabes de 2011, les cyberdissidents ont malgré tout réussi à rester en contact avec le monde extérieur. L'appui des grandes entreprises, le plus souvent américaines, comme Twitter et Facebook (sans oublier le soutien plus discret d'ONG ou de services d'État) y a contribué largement en Egypte par exemple. Cette porosité relative[43] du cyberespace en fait ainsi le lieu privilégié de la propagande et des opérations psychologiques[44].

Le conflit entre Israël et le Hezbollah en 2006 montre comment la stratégie asymétrique de l'organisation chiite s'est focalisée sur la mise en scène, *via* le cyberespace, de l'échec patent des opérations militaires israéliennes. Comme les forces nord-vietnamiennes lors de l'offensive du Têt de 1968, les responsables du Hezbollah ont voulu transférer le conflit d'un domaine militaire pur vers un domaine politico-médiatique. Avec les cyber-outils à leur disposition, ils ont cherché à propager dans l'opinion publique israélienne, des pays arabes et jusqu'en Occident, l'idée que les opérations militaires israéliennes, contrairement à ce

[42] En termes militaires américains: *full spectrum operation.*
[43] Il est évident qu'un pays comme la Chine exerce un contrôle *intra muros* bien plus efficace sur les réseaux sociaux que la Tunisie ou la Turquie.
[44] Les opérations psychologiques – qui dans la pensée stratégique américaine incluent aussi les opérations informationnelles – sont définies dans le FM 3.5-30 de l'armée américaine comme un appui essentiel aux opérations militaires.

qu'affirmait Tsahal, étaient tenues en échec dans de nombreux endroits. Il s'agit d'une illustration du principe clausewitzien : dans les conflits contemporains, en particulier ceux qui ont une dimension cyber, la victoire consiste de plus en plus à faire croire à l'autre ou à l'opinion que l'on a gagné. La rhétorique de la résistance patriotique du Hezbollah défendant le sol du Liban après que l'armée libanaise se soit retirée a également contribué à cet effet. Cette cyberpropagande, poursuivie après les actions militaires pour mettre en scène le « triomphe » du parti de Dieu, a permis au parti chiite de capitaliser sur son succès militaire pour devenir ensuite la première force politique du Liban.

Des exemples récents montrent l'action sur les perceptions *via* le cyberespace, intégrée aux opérations militaires traditionnelles. Ainsi Tsahal, tirant les leçons de son échec de 2006, a développé une stratégie innovante, notamment au travers des réseaux sociaux. Lors de l'opération Pilier de Défense en novembre 2012 dans la Bande de Gaza, Tsahal utilise massivement des comptes Twitter en différentes langues[45] pour riposter à la propagande palestinienne[46], fournir des arguments à ses propres partisans et attirer les médias ou l'opinion des pays tiers vers des images ou des pages favorables à son « grand récit »[47].

La mise en scène et en ligne de ses propres victoires ou des échecs des adversaires est devenue une composante de la stratégie militaire. Le piratage d'un drone Sentinel américain en 2011 par les forces iraniennes a ainsi été exploité par ces dernières pour démontrer leurs propres capacités technologiques, mais aussi l'impéritie des Américains, trop dépendants du matériel. Alors que les drones, objets d'un important débat stratégico-éthique, sont devenus l'une des armes préférées des Etats-Unis, les Iraniens, en contestant leur fiabilité au travers d'une cyberpropagande efficace[48], ont relancé le débat sur leur utilisation.

Loin de la cyberguerre annoncée dans les années 1990 par les analystes américains – Arquilla et Ronfeldt p.e. – et, au-delà, d'un appui cyber technique direct aux opérations militaires (pertubation de matériels, brouillage des communications, désactivation de systèmes de défense), c'est bien l'action sur les perceptions qui domine aujourd'hui. La facilité d'accès,

[45] Israël s'exprime sur Twitter et Facebook, mais aussi Pinterest et Tumblr. Trois comptes twitter sont créés : @FDISpokesperson, @Tsahal_FDI, @FDIonline (le second étant en français et le dernier en espagnol)
[46] Les groupes palestiniens répondent (notamment les Brigades Ezzedine al-Kassam (la branche armée du Hamas) @AlqassamBrigades) par des tweets et donnent leurs comptes-rendus de tirs de roquettes.
[47] « nous sommes l'armée d'un pays démocratique qui ne fait que se défendre contre des attaques terroristes et s'efforce d'éviter toute victime innocente ».
[48] Cette dernière mêle déclarations officielles, images télévisuelles et communiqués des agences de presse du régime présentes sur Internet comme IRNA.

l'interconnexion croissante, l'immédiateté et les problématiques liées au contrôle de l'information déterminent ces opérations avant tout psychologiques.

12 Le retour de l'État

Le cyberespace, loin de concrétiser la fin annoncée des frontières – rhétorique commune à la mondialisation – a vu les États se renforcer dans leurs capacités souveraines, à commencer par les occidentaux et principalement les Etats-Unis qui en sont à l'origine. L'affrontement géopolitique autour du contrôle et de la normalisation internationale du cyberespace est le reflet de cette ambition géopolitique des États. Les caractéristiques du cyberespace, comme la question de la non-attribution ou la difficulté de définition et de représentation du territoire national dans cet espace, leur laissent une grande marge de manœuvre.

La question de la viabilité des alliances étatiques – OTAN par exemple – lors de cyberconfrontations reste ouverte. Ainsi en Estonie en 2007, une application de l'article 5 du Traité de l'Atlantique Nord fut évoquée. Les critères du seuil de conflictualité dans le cyberespace et l'origine de l'agression n'étant pas clairement définis, l'Alliance atlantique n'a pu soutenir un de ses membres en difficulté. Le 14 juin 2007, une réunion des ministres de la défense de l'Alliance à Bruxelles aboutit à une déclaration sur le renforcement des capacités de l'OTAN en matière de cyberdéfense qui ne préguge pas définitivement de la posture à adopter en cas de cyberagression.

La confrontation américano-chinoise se transcrit aussi dans le cyberespace où l'impossibilité d'une attribution certaine confère une forme d'impunité à ceux qui y agissent. Les Etats-Unis sont la principale cible des grandes agressions à visée géopolitique[49]. La plupart sont des actions d'espionnage classique utilisant les moyens techniques du cyberespace, ce qui replace l'élément informationnel et cognitif au cœur de la stratégie de puissance.

La conflictualité géopolitique dans le cyberespace laisse une place très importante aux acteurs non-étatiques. ONG, groupes terroristes ou associations diverses, comme les Talibans afghans et autres groupes pratiquant le cyber-jihad contre les intérêts occidentaux (bancaires notamment) profitent du « pouvoir égalisateur » qui permet d'agir plus facilement que dans le

[49] Les opérations Aurora (2009), Octobre Rouge (2007), le vol des données du F-35 (2005-2011), Titan Rain (2003-2005) ainsi que les actions de l'Armée électronique syrienne en 2012-2014 visent directement les Etats-Unis.

domaine physique et d'avoir plus d'écho par des stratégies de subversion et d'agit-prop. Ce pouvoir est donc plus sémantique que technique.

Les États trouvent également dans le cyberespace de nouveaux moyens d'action. Les Etats-Unis eux-mêmes, s'ils sont la principale cible, semblent également être le principal acteur. L'affaire PRISM découverte en juin 2013 révèle l'ampleur de cette action, même si PRISM n'est qu'une version beaucoup plus avancée du programme Echelon de la fin des années 1990, déjà destiné à surveiller les communications mondiales à des fins géopolitiques[50]. D'autres grandes puissances, ou aspirant à l'être, tendent à se doter de telles capacités soit en collaborant avec les Etats-Unis (Allemagne, Royaume-Uni) soit par elles-mêmes (Chine, Russie). La révélation de l'implication des Etats-Unis et d'Israël dans l'affaire Stuxnet est un exemple d'offensive étatique non-militaire dans le cyberespace, révélée par le New York Times en juin 2012 et confirmée par E. Snowden en 2013.

Dans la rivalité entre les deux Corées, ravivée depuis l'accession au pouvoir de Kim Jong-Un, l'agression Dark Seoul du 20 mars 2013 marque une nouvelle étape. Si la Corée du Nord nie officiellement sa participation, les agences de sécurité sud-coréennes désignent le voisin du nord comme responsable. Il s'ouvre ainsi une « zone grise » dans les relations géopolitiques où un cyberaffrontement limité devient plus qu'envisageable, du fait de sa rentabilité et de son impunité, surtout quand l'exploitation sémantique n'est pas le fait de l'agresseur cherchant à montrer sa puissance. A l'exception de quelques États occidentaux, dont les Etats-Unis, peu de pays ont fait état de leur doctrine cyber et de leurs capacités offensives. Sur fond d'incertitudes, c'est en réalité un retour au premier plan de l'État qui est en train de se produire.

13 La cyberconflictualité économique

Longtemps oubliée voire niée, la conflictualité économique s'étend aussi dans le cyberespace. La financiarisation et la tertiarisation croissante des économies du Nord ont rendu les entreprises plus sensibles aux effets d'image. En effet la mondialisation des marchés financiers a renforcé le caractère transnational des entreprises : elles sont devenues des actifs économiques s'échangeant dans les bourses mondiales. Les premiers acteurs économiques

[50] Né de la lutte contre le bloc soviétique, le système Echelon était déjà sensé, dans la décennie 1990, servir à la lutte contre le terrorisme, la prolifération des armes de destruction massive, les trafics internationaux, etc., même si beaucoup y voyaient un dispositif d'espionnage économique.

mondiaux sont aujourd'hui les fonds spéculatifs ou d'investissement étatiques comme les fonds souverains ou privés comme les *hedge funds*. La mondialisation a ainsi créé un entrelacement des marchés et des acteurs économiques.

Dans ce cadre, le *goodwill*[51] prend une telle importance que certaines entreprises ne reposent quasiment plus que sur celui-ci, telles certaines banques ou des grands acteurs de l'Internet comme Facebook. Par voie de conséquence, les entreprises deviennent de plus en plus sensibles à l'image et cherchent à la protéger, en se souciant par exemple de leur e-réputation, d'où la tentation pour un rival de s'en prendre à l'image de l'entreprise ciblée, pratique parfois désignée sous le vocable de « guerre informationnelle ».

La cyberconflictualité économique consiste souvent en l'exploitation maligne de l'information pour faire baisser des cours de bourse (agression de l'Armée électronique syrienne contre le compte Twitter de l'Associated Press), pour faire perdre des marchés (GDF-SUEZ au Brésil dans l'affaire du barrage de Jiraù), pour faire échouer des négociations (Climategate), dans le but d'amoindrir la puissance économique de l'adversaire. La vitesse compte alors beaucoup, comme dans le cas d'investisseurs boursiers réagissant en temps réel à une information négative[52]. La vitesse de circulation de l'information combinée à de nouveaux cyber-outils de *trading* comme le *High Frequency Trading* peut provoquer une mini-crise boursière[53]. D'un autre côté la révélation, un mois avant la conférence climatique de Copenhague en 2009, d'informations tirées d'e-mails de climatologues réputés a partiellement discrédité les travaux scientifiques servant de base à ces négociations. L'enjeu économique non-négligeable derrière ce Climategate (comme l'a nommé la presse anglo-saxonne), induit une opération complexe et séquencée, utilisant des blogs et des sites spécialisés. Dans les deux cas le poids de l'information dans le domaine économique a été largement démontré.

Le travail sur les perceptions effectué à l'occasion de ces manœuvres, l'une de désinformation (AES), l'autre de déception en exploitant des informations vraies (Climategate) met en avant l'importance de l'appréhension de l'information par le monde économique. Certes, les

[51] Valorisation comptable des actifs immatériels de l'entreprise incluant l'image et la réputation.
[52] Ainsi pour l'attaque contre Associated Press Un vol de mot de passe de son compte Twitter par l'Armée électronique syrienne a permis la propagation de la fausse nouvelle d'un attentat contre la Maison Blanche. Dans les vingt minutes qui ont suivi, l'indice *Dow Jones* a perdu 143 points, soit une perte de 136 milliards USD environ.
[53] De même en septembre 2013, un délit d'initié à la bourse de Chicago a abouti au détournement de 800 millions USD en 7 millisecondes à la suite d'une annonce de la Réserve Fédérale américaine.

techniques utilisées ne sont pas nouvelles – pour la plupart elles ont été créées entre la fin du XIX^{e} et le milieu du XX^{e} siècle –, mais elles étaient avant l'apanage des domaines politique et militaire. Leur banalisation dans le domaine économique reflète et l'importance prise par l'image dans l'économie occidentale, et le rôle des technologies de l'information et de la communication.

Les agressions contre le domaine économique peuvent être revendiquées et certaines devenir l'objet de manœuvres de subversion à travers la révélation de leur but ou de leur source. Les affaires Titan Rain de 2003-2005, Luckycat de 2009-2011 et le vol des données du F-35 depuis 2007 sont des cas de revendication/désignation. À ce titre, le domaine économique ne diffère pas des domaines militaire et géopolitique, même si les mesures de protection sont souvent moindres. Cela peut amener la réorientation d'actions géopolitiques vers les entreprises, cibles plus faciles à attaquer comme le montre l'opération OpGabon des Anonymous qui s'est réorientée vers les grandes entreprises présentes au Gabon[54] après les échecs initiaux contre les cibles étatiques. De même, le contrôle bien moindre que les entreprises effectuent sur la provenance des matériels utilisés ouvre de nouvelles vulnérabilités qui ont été résolues dans les domaines géopolitique et militaire. Le vol des données du F-35 le démontre : la vulnérabilité est venue d'un fournisseur, en l'occurrence celle des *tokens* d'accès à distance au système informatique central de Lockheed-Martin utilisés pour le télétravail.

Comparé aux domaines militaire et géopolitique, le domaine économique reste relativement secondaire[55]. Ce constat peut être relativisé notamment parce que de nombreuses agressions informatiques réussies contre de grandes entreprises ne sont pas rendues publiques précisément pour éviter une atteinte à leur image. La récente montée en puissance de ce type d'agression dépend de facteurs technologiques (la présence accrue des entreprises dans le cyberespace, leur dépendance à l'égard des réseaux, le développement des parcs informatiques fixe et mobile) et de facteurs économiques (interconnexion des bourses, mondialisation des capitaux, caractère transnational des entreprises). La multiplication des cas depuis le milieu des années 2000 traduit une augmentation de la cyberconflictualité économique avec une utilisation directe ou indirecte de la couche sémantique. Dans les trois domaines, les études de cas montrent que les cyberagressions s'articulent de manière spécialisée comme de manière combinée. D'où une véritable transversalité.

[54] Notamment la filiale locale de l'assureur Axa.
[55] Sur les 38 cas étudiés, seuls 5 sont purement économiques et 5 autres peuvent compter un volet économique.

II Vers la transversalité ?

La transversalité des actions qui trouve son origine dans une égalité d'accès aux cibles dans le cyberespace tend vers des actions à la confluence des domaines géopolitique, militaire et économique.

L'utilisation de l'économie à des fins d'accroissement de puissance par les États et l'imbrication croissante entre État et entreprises, notamment dans les pays émergents, amènent à s'interroger sur la porosité entre ces deux univers. Ainsi la remise en avant du concept de capitalisme d'État (notamment chez Rodrik ou Stiglitz) rapproche les sphères économique et étatique. De même, le cyberespace étant, avant tout, un espace de perceptions, une entreprise ou un acteur économique y est avant tout identifié par sa nationalité réelle ou supposée et par sa relation avec un gouvernement.

Ainsi la cyberagression Shamoon contre Aramco qui appartient à la famille royale saoudienne et représente le principal actif économique du pays, semble viser tant des intérêts économiques que politiques. En effet, la compagnie possède la quasi-intégralité des réserves pétrolières saoudiennes et réalise un chiffre d'affaires de plus de 400 milliards USD par an. La revendication de cette agression par le groupe Epée Tranchante de la Justice aussi bien que la nature du maliciel employé[56], suggèrent une action contre la politique extérieure du régime saoudien. Shamoon serait une agression transversale au confluent des éléments économique et géopolitique, thèse qui serait encore renforcée s'il était prouvé que l'Iran en est bien l'organisateur direct ou indirect. De même les vols de données liées à des programmes militaires, directement chez les industriels de défense comme Lockheed-Martin, premier fournisseur de l'armée américaine, s'apparentent à une agression tant économique que géopolitique.

La coopération entre État et entreprises, même hors d'un cadre de capitalisme d'État, se révèle cruciale en cyberstratégie. L'affaire PRISM soulève la question de la coopération entre les grandes entreprises de l'Internet comme Google, Facebook, Twitter ou Yahoo et les autorités politiques dans des buts géopolitique et économique. Les entreprises qu'elles appartiennent ou non au domaine de l'information, sont devenues la vitrine des États et donc

[56] Shamoon après avoir infecté un système fait apparaître un drapeau américain en train de brûler.

des cibles privilégiées pour les toucher, *in fine*. L'opération OpGabon des Anonymous visait ainsi, en second ressort après l'échec d'une première phase tournée vers les actifs étatiques gabonais, les filiales locales d'entreprises occidentales. L'idée était d'amener leurs pays d'origine à se positionner par rapport à la dénonciation des crimes rituels. Attaquer une entreprise peut n'être que la première étape pour atteindre un État tout comme une cyberagression sémantique sur des forces militaires peut servir à discréditer l'autorité politique qui les contrôle (Israël-Hezbollah).

Il n'est pas rare de constater une exploitation géopolitique d'actions relevant du champ militaire qu'il s'agisse du piratage de drones pour montrer qu'ils espionnent en territoire souverain (drone Sentinel en Iran) ou de la mise en avant de difficultés militaires d'une armée pour atteindre le moral de la population (Israël-Hezbollah, Israël-Hamas, OTAN au Kosovo). En démontrant l'iniquité ou l'inutilité de l'attaque militaire, les attaquants espèrent agir sur les populations des pays adverses, surtout s'ils sont démocratiques. Même dans des agressions comme l'Opération verger, l'exploitation de l'ensemble de l'attaque contre la Syrie relève plus du domaine géopolitique en servant, dans ce cas, à montrer la détermination d'Israël face à des antagonistes susceptibles de franchir un seuil technologico-militaire[57], ainsi qu'à prouver ses capacités d'intervention purement militaires. Il en est de même pour la guerre de 2008 entre Russie et Géorgie : elle a avant tout servi à la Russie à lancer un message à l'Occident sur son engagement dans le Caucase et sa résolution à contrôler cette région qui fait partie de « l'étranger proche »[58].

Si les agressions combinées transversales restent minoritaires[59], elles tendent à se multiplier. La complexité des relations entre les trois domaines d'action stratégique ou leur enchevêtrement sont patents. L'utilisation de technologies dites « duales » en est la meilleure preuve comme dans l'affaire Conficker de 2009 : la faille exploitée était commune aux systèmes d'exploitation et de serveurs Microsoft utilisés aussi bien dans les armées que dans les entreprises. Le cyberespace apparaît comme un lieu de la conflictualité transverse particulièrement délicat à appréhender pour des acteurs monolithiques comme les États.

[57] Principalement l'acquisition de technologies nucléaires.
[58] L'étranger proche regroupe l'ensemble des pays qui ont été sous la tutelle prolongée de la Russie en Europe (Ukraine, Biélorussie), dans le Caucase (Géorgie, Azerbaïdjan, etc.) ou en Asie centrale (Kazakhstan, Kirghizistan, etc.). La Russie considère cette zone comme son lieu d'intérêt et d'influence prioritaire et met en avant sa volonté d'y intervenir.
[59] Sur les 38 cas étudiés, 27 restent des agressions ne visant qu'un des trois types de cible.

Chapitre 3 - Internationalisation et sélection des alliances

Une des notions indispensables pour décrire le système international est celle d'alliance. Leur construction dans le cyberespace diffère de la pratique traditionnelle, d'où une nouvelle typologie des alliances.

I Spécificité des alliances dans le cyberespace

Nouer des alliances répond à des besoins et des intérêts bien identifiés. Or, la nature du cyberespace change les critères classiques.

11 Nature des alliances

Une alliance est fondée principalement sur la base d'un calcul d'un rapport de force. Ce calcul est toujours approximatif faute de mesurer la puissance de l'adversaire. Chacun évalue la sienne et celle de l'autre. Ceci s'est longtemps fait à partir d'indicateurs visibles : nombre d'hommes, équipements, détention d'arme nucléaire, évaluation de la capacité tactique et de la valeur morale des unités. Les calculs stratégiques des uns et des autres étaient fondés sur une base à peu près partagée.

Les alliances défensives visent à la dissuasion, supposée éviter l'emploi de la force, quand les alliances offensives modifient le rapport de forces dans une perspective d'emploi éventuel. Ces alliances sont habituellement circonstancielles car elles varient dans le temps selon les intérêts des parties. La guerre moderne a souvent favorisé une configuration binaire où chacun tend à construire ses alliances en fonction de son intérêt propre et de l'équilibre général.

Il existe d'autres critères que le défensif et l'offensif : permanence (alliance temporaire ou durable), nombre d'acteurs (alliances bilatérales ou collectives), proximité géographique (alliance contiguë ou distante), forme juridique (alliance formelle ou objective, parfois dite tacite), étendue des obligations contractées (alliance précise ou générale) et structuration de l'alliance (organisation fluide ou structurée).

12 Critères des cyberalliances

Le rapport de force est difficile à mesurer. Certes, il existe des critères objectifs tels le degré d'informatisation de la société, le taux d'infrastructure cyber, la taille et la dimension des acteurs économiques du cyberespace, la mise en place d'une cyberstratégie et d'une organisation de cyberdéfense. Mais le critère quantitatif a peu de sens dans le cyber. Or, cette visibilité des moyens n'existe pas dans le cyberespace où chacun peut se dissimuler. Chaque acteur peut celer son degré réel de cyberpuissance puisque les capacités ne dépendent pas du nombre d'ordinateurs mais de l'ingéniosité des spécialistes. Chaque acteur peut aussi leurrer sur ses capacités.

Le cyberespace est non-contigu. Jusqu'alors, on s'alliait principalement avec des puissances voisines ce qui facilitait le secours réciproque. Une des grandes difficultés de l'Alliance atlantique tient à l'éloignement fondateur entre les deux rives de l'océan et donc la distance géographique entre l'allié le plus puissant et les autres. Avec le cyber la distance importe peu. Si chacun est voisin, la proximité n'est plus un critère de choix des alliances.

L'un des principes stratégiques du cyberespace réside dans l'inattribution des actions qui ne facilite pas l'identification de l'ennemi et de l'ami. Ceci favorise des logiques « tous azimuts », conformément au discours français sur la dissuasion[60]. Chacun peut désormais agir contre n'importe quel acteur sans s'exposer automatiquement à une rétorsion.

Il est tentant d'espionner le voisin pour savoir ce qu'il sait, ce qu'il cache et ce dont il est capable. Un acteur puissant peut expliquer à ses alliés qu'ils ne sont pas au niveau pour les amener à révéler leurs capacités. Cela pose la question de la coopération qui accompagne normalement toute alliance. Sous couvert de partage technique, l'un des alliés peut apprécier plus précisément la valeur technique de l'autre. S'allier dans le cyber implique un risque, celui qui fait ce choix dissipe l'opacité relative qui protégeait.

Dans le cyberespace, les alliances se nouent avec les acteurs avec lesquels on peut partager ses forces et surtout ses vulnérabilités, son vrai secret. Dans le système traditionnel, une alliance vise à réunir des forces, dans le cyberespace, elle sert surtout à partager des faiblesses.

[60] Charles Ailleret, « "Défense "dirigée" ou défense "tous azimuts" », *Revue de défense nationale*, décembre 1967.

Dans le cyber, les intérêts portent moins sur des objectifs matériels ou territoriaux, mais sur des ressources et des informations. À considérer le seul cyberespace, la confiance devient le nouveau critère pour constituer une alliance. Les alliances se déterminent moins contre une puissance menaçante qu'avec une puissance de confiance pour partager des vulnérabilités plus qu'additionner des forces.

II Typologie des alliances dans le cyberespace

21 Alliances étatiques

Les alliances étatiques peuvent être **multilatérales**, même s'il y a peu d'exemples avérés : ainsi, l'OTAN ou l'UE.

L'Alliance atlantique a réellement pris conscience de cette thématique à partir de l'agression contre l'Estonie en 2007. La mise en œuvre de l'article 5[61], un moment évoquée, n'a pas eu lieu. Le champ de la cyberdéfense fut incorporé au concept de 2010 accompagné d'une politique de cyberdéfense, de la création d'un centre OTAN de réponse aux crises (NCIRC) et d'une section cyber au Secrétariat international. De même, un centre d'excellence OTAN de cyberdéfense fut créé par l'Estonie à Tallinn avec la participation de nombreux alliés. Toutefois, ce centre n'appartient pas à la structure intégrée ce qui limite son influence.

Les alliés sont d'accord pour que l'Alliance organise son autodéfense, c'est-à-dire la cyberdéfense de l'organisation. En revanche, celle-ci n'entre pas dans le périmètre de la défense collective. Pour les alliés les plus avancés technologiquement, l'intervention de l'Alliance dans leur cyberdéfense, au cœur de leur souveraineté, supposerait un partage des faiblesses et des secrets avec tous membres. Or, cette perspective n'est pas admissible puisque certains alliés n'ont fait quasiment aucun effort en la matière. L'Alliance se voit donc cantonnée à un rôle restreint mais peut constituer un cadre pour la formation partagée. Elle peut également servir de laboratoire pour des actions cyber coordonnées avec des opérations militaires classiques, rentrant bien, cette fois, dans la fonction d'alliance militaire de l'OTAN.

[61] L'article 5 du Traité de l'Atlantique Nord est au cœur du dispositif puisqu'il prévoit la défense collective.

L'Union européenne[62] a longtemps ignoré le domaine. Puissance civile, elle n'est guère orientée vers la défense en dépit d'une politique de défense et de sécurité commune (PSDC) actée dans le traité de Lisbonne. Elle doit résoudre trois dilemmes : entre l'intérêt communautaire et les intérêts nationaux, entre la logique du bien public et les intérêts privés, entre le principe de concurrence et celui de sécurité.

C'est pourquoi la « Stratégie de cybersécurité de l'UE », publiée en février 2013, a constitué une heureuse initiative articulée autour de plusieurs instruments (ENISA, CERT, EC3/EUROPOL). Cette démarche constitue un premier pas. L'intérêt de l'UE pour ces sujets a été relancé à partir de l'été 2013 par le scandale PRISM. Si la Commission a minimisé la chose, le Parlement a été plus préoccupé et a posé la question des accords Swift ou de la nécessité de négocier le TTIP[63]. Il faut de même mentionner les initiatives allemandes comme le projet de logiciels européens face aux systèmes américains.

Les Five eyes du réseau Echelon[64] sont une alliance anciennement établie, d'abord pour le renseignement électromagnétique puis étendue à l'ensemble du cyberespace. Elle réunit cinq acteurs (Etats-Unis, Royaume-Uni, Australie, Canada, Nouvelle-Zélande) depuis les années 40.

Le faible nombre d'alliances multilatérales tient moins à la nouveauté du cyberespace qu'il semblerait. Soit le partage des informations s'effectue en bilatéral pour réduire la possibilité de fuites, soit le partage est restreint et cela permet de passer en multilatéral.

Les alliances étatiques peuvent également être **bilatérales**.

L'alliance Etats-Unis - Israël : l'affaire Stuxnet est un tournant dans la prise de conscience de la cyberconflictualié. Pour la première fois, une cyberarme avancée est employée par des États contre un autre État, l'Iran. S'il n'y a pas de preuves absolues que les auteurs de l'attaque aient été les Etats-Unis et Israël, de nombreuses indiscrétions et éléments techniques permettent de les désigner. Les conditions géopolitiques expliquent une telle alliance pour empêcher l'Iran de développer ses recherches nucléaires. Le retard provoqué par la

[62] Voir O. Kempf, « La cyberstratégie de l'Union Européenne », *Sécurité Globale* n° 24 (été 2013), p 25-40.
[63] Les accords Swift portent les échanges d'informations bancaires quant au Transatlantic Trade and Investment Partnership, il s'agit d'un partenariat de commerce et d'investissement, toujours en cours de négociation entre l'UE et les Etats-Unis.
[64] Voir Claude Delesse, « *Echelon et le renseignement électronique américain* », Editions Ouest-France, 2012. De même, Jean Guisnel, « *Guerres dans le cyberespace* », Editions La Découverte, 1997.

cyberagression évitait de recourir à la frappe physique directe contre les installations iraniennes, au moins pour quelques temps. Cela permettait en particulier de retarder une éventuelle frappe israélienne. Cette alliance ponctuelle permettait à chacun des acteurs de conserver son autonomie stratégique.

L'alliance entre Etats-Unis et Royaume-Uni a été révélée à l'occasion de l'affaire PRISM. Ainsi, le programme Tempora[65] montre que cette coopération est beaucoup plus poussée et structurelle. Les révélations de Snowden ont permis de rendre publique l'ampleur de la coopération entre la NSA et le GCHQ, au point que cela soulève des interrogations sur la capacité résiduelle d'autonomie stratégique de l'acteur britannique. La domination des Etats-Unis sur le Royaume-Uni était déjà patente dans d'autres domaines comme le nucléaire avec les accords de Nassau.

Concernant les rapports entre l'Iran et le Hezbollah, ceux-ci sont si intenses que l'on hésite à parler d'alliance ou de sujétion.

En Europe, le Livre Blanc français de 2013 affirme que « *Toute politique ambitieuse de cyberdéfense passe par le développement de relations étroites entre partenaires internationaux de confiance. Les relations seront approfondies avec nos partenaires privilégiés, au premier rang desquels se placent le Royaume-Uni et l'Allemagne. Au niveau européen, la France soutient la mise en place d'une politique européenne de renforcement de la protection contre le risque cyber des infrastructures vitales et des réseaux de communications électroniques* » (p. 107). C'est ce que confirme le ministre de la Défense à Rennes le 3 juin 2013 lorsqu'il déclare : « *Enfin, le développement de relations étroites avec nos principaux partenaires étrangers devra être soutenu* ».

PRISM a une apparence multilatérale puisqu'il est constitué sur la base des Five eyes, mais il semble avoir été renforcé par trois coopérations en matière d'échange de renseignement avec la France, l'Allemagne et la Suède, à en croire les révélations de la presse.

22 Alliances hybrides

Dans cette configuration, un des acteurs est un Etat, l'autre ne l'est pas. Tous les cas de figure sont envisageables : État engageant ou subventionnant des acteurs privés, militants ou

[65] Sous-partie de PRISM : le prélèvement dit *upstream* de données dans les câbles sous-marins.

soutenant des cyberdissidences ; État s'alliant avec une société privée soit pour un système d'espionnage ou de surveillance soit pour soutenir des mouvements politiques extérieurs ; grande entreprise du Net affirmant hautement ses choix en politique étrangère, négociant avec des gouvernements, les menaçant, soutenant des groupes militants.Une société comme Google peut être tantôt aux côtés des cyberdissidents, tantôt attaquée par d'autres militants, tantôt coopérant avec la NSA, tantôt victime d'espionnage étatique.

Le cas des alliances Etat-entreprise est fréquent. En matière de coopération directe, on pense à l'affaire Megaupload ou au soutien de l'État français à Areva. De même, les affaires d'espionnage Aurora, Titan Rain ou F-35 ont été attribuées à la Chine au profit de son économie. Il en est de même pour Octobre rouge, opération d'espionnage économique qui proviendrait de Russie.

L'entreprise peut aussi agir au profit de l'État. L'affaire Snowden s'est ouverte sur le scandale Verizon, suivi par la révélation de la façon dont les grands acteurs de l'Internet, en particulier les GAFA collaboraient avec les autorités américaines.

Les États peuvent nouer des alliances avec des acteurs collectifs : soutien américain aux cyberdissidents arabes, rapports entre l'AES et Damas, rapports entre le Russian Business Network et Moscou.

Des Etats ont encouragé les initiatives venues de simples internautes : agressions de patriotes serbes contre l'OTAN en 1999, de hackers patriotes russes contre l'Estonie en 2007 ou la Géorgie en 2008.

Chapitre 4 - Règles, normes et standards

Les acteurs peuvent affecter l'environnement de deux façons : soit en passant par une normalisation technique, soit par une régulation juridique.

I Règles, normes et standards techniques

Le cyberespace reste le seul espace stratégique artificiel permanent fondé par l'homme sur des normes techniques qui l'autorisent et le pérennisent. Pour cette raison, la bataille d'influence autour de normes est un enjeu majeur de la géopolitique de l'Internet et cela amène les États comme les entreprises à s'intéresser de plus en plus à la question technique.

11 Le contrôle par la norme

111 prédominance américaine

Le cyberespace qui est né de la volonté de l'État américain est resté rattaché à ce dernier à travers la technologie. Les normes techniques qui fondent le cyberespace sont ainsi issues du corpus normatif américain. L'une des plus connues est le code ASCII (American Standard Code for Information Interchange) qui a longtemps été la base de la transcription des textes dans le cyberespace. Il traduisait la primauté de l'alphabet latin et, en plus, de la graphie américaine puisqu'il ne reconnait pas les caractères accentués. La plupart des protocoles et des normes existant à l'heure actuelle dans le cyberespace sont ainsi issues des Etats-Unis ou d'entreprises américaines que ce soit le protocole TCP (TCP/IP aujourd'hui) développé pour l'Arpanet ou même l'OSI (Open Systems Interconnection) combattue par les opérateurs européens lors de son adoption par l'ISO comme norme internationale en 1977. À l'heure actuelle les principaux organismes normatifs, agissant souvent selon un modèle de *soft law*, sont fortement affiliés aux Etats-Unis. L'IEEE (Institute of Electrical and Electronic Engineers), responsable de la création de la norme WiFi, bien que se présentant comme une association internationale, reste une société de droit américain formée par la fusion des associations d'ingénieurs électroniciens des Etats-Unis. Au niveau international, les Etats-Unis jouent un rôle moteur au sein de l'ISO – l'IEEE a eu un rôle important dans sa création – et sont à l'origine de l'ISA (International Society of Automation) qui a élaboré, entre autres, une des normes internationales de cybersécurité des SCADA, ISA99.

112 Géopolitique normative et balkanisation du cyberspace

La question de la promotion de normes particulières dans le cyberespace renvoie à la géopolitique des normes. De nombreux États tentent d'imposer leurs vues techniques pour sortir du monopole américain. La bataille qui a eu lieu dans les années 2000 autour de la possibilité de créer des noms de domaine en caractères non-latins illustre bien cette problématique. Depuis octobre 2009, l'ICANN autorise les noms de domaines internationalisés en arabe, cyrillique et chinois, mettant fin au monopole de l'alphabet latin. Même si la part des noms de domaine en alphabets non-latins reste limitée – il existait au début de 2014 environ 900 000 noms de domaine russes en cyrillique contre 5 millions en alphabet latin[66] – leur popularité n'est plus à démontrer. Il s'agit là d'une manœuvre technique internationale contribuant à ce qui est qualifié péjorativement de balkanisation du Net et par laquelle les cultures dominantes non-latines, notamment chinoise et russe, cherchent à gagner leur autonomie. La balkanisation qui s'instaure dans les normes de l'ICANN renforce la position des pays émergents dans le cyberespace où ils deviennent des acteurs incontournables. Ainsi en 2012 la Chine est devenue le premier utilisateur mondial de plateformes mobiles, tablettes et smartphones.

Si la primauté américaine dans le domaine des normes techniques n'est plus à démontrer, le monopole occidental est de plus en plus remis en cause. La Chine a entrepris une stratégie globale très en amont en tentant de créer un espace séparé proprement chinois. Pékin a ainsi développé une barrière technique aboutie, la Grande muraille de feu, pour contrôler l'accès de ses internautes aux sites localisés hors du pays. La Chine a encouragé la création d'équivalents de tous les sites web populaires au niveau mondial, ce qui l'a mise en position de force notamment face à Google en 2010. Il existe des équivalents de Google (Baidu), Facebook (Renren), Twitter (Weibo), YouTube (QiYi), etc. La Chine impose un contrôle technique sur sa population – qui se combine par ailleurs à un contrôle humain – dans le but avoué de la protéger des influences extérieures. S'il n'est pas encore capable d'agir sur la structure même de l'Internet largement sous influence américaine (serveurs racine, ICANN), ce contrôle technique à un niveau secondaire national permet une certaine fermeture du territoire et dément encore nombre de prophéties sur la façon dont Internet balaierait l'isolement informationnel des pays autoritaires et ridiculiserait toute tentative de censure.

[66] T. Golovanova, « Un nouveau nom de domaine russe en cyrillique » sur Russia Beyond the Headlines : http://fr.rbth.com/en_bref/2014/01/10/un_nouveau_nom_de_domaine_russe_en_cyrillique_27355.html ; consulté le 24/03/2014.

La diffusion mondiale de produits chinois, des routeurs de cœur de réseau aux terminaux mobiles, élargit l'influence chinoise et les capacités techniques d'intervention sur les réseaux.

113 L'action des acteurs privés

De nombreux acteurs se positionnent graduellement dans le domaine technique en cherchant à transformer leurs solutions technologiques en normes internationales. Les entreprises sont très actives en ce domaine et tentent, le plus souvent par effet de masse, de transformer leurs technologies en normes universelles. Ce fut par exemple le cas du Bluetooth développé par Ericsson qui devint norme globale après la formation du Bluetooth Special Interest Group[67] par Ericsson, IBM, Intel, Toshiba et Nokia en 1998. De même la technologie USB est issue du regroupement entre Microsoft, Compaq, NEC, Intel, IBM et Northern Telecom en 1996. Dans ces deux cas, les membres de ces alliances appartiennent à l'ensemble du spectre des entreprises du cyberespace : des constructeurs de composants (Intel, NEC), de matériels pour particuliers ou entreprises (IBM, Compaq, Ericsson), des développeurs de logiciels (Microsoft). Le développement de nouvelles technologies capables de devenir des normes passerait ainsi par la création d'alliances larges impliquant des acteurs tout au long de la chaîne.

Cette tendance se heurte à la concentration des acteurs. Dans le domaine des semi-conducteurs, l'américain Intel occupe à lui seul plus de 15 % du marché mondial, loin devant ses concurrents, à tel point qu'il est souvent poursuivi pour abus de position dominante[68]. La concentration des acteurs technologiques leur permet ainsi de peser sur l'élaboration de normes internationales en créant des produits que leur développement auprès du grand public ou d'un grand nombre d'entreprises, transforme *de facto* en normes techniques globales. Ainsi de nombreuses normes de fichiers sont ainsi issues de la pratique de Microsoft et de ses logiciels (Windows, Office).

12 Universalité technique

Les cas analysés montrent qu'il n'existe pas de cyberarme absolue. En effet, toute cyberarme est conçue pour affecter un certain système et même, à l'intérieur de ce dernier, pour ne s'attaquer qu'à une vulnérabilité particulière. Néanmoins certaines vulnérabilités peuvent se

[67] https://www.bluetooth.org/en-us ; consulté le 28/05/2014.
[68] http://www.liberation.fr/economie/2009/05/13/amende-record-pour-intel_557702 ; consulté le 28/05/2014.

révéler particulièrement graves à la mesure de leur caractère critique ou de la popularité du système visé. En lui-même, le maliciel Conficker n'est pas très dangereux ; il est relativement simple techniquement – du moins dans ses premières versions A et B – et ne cause pas de dommages insupportables : tout au plus bloque-t-il l'action des anti-virus et les mises à jour. Sa réelle force vient plutôt du fait qu'il s'attaque aux systèmes d'exploitation de Microsoft (Windows et Windows Server), les plus répandus au monde, chez les particuliers, dans les entreprises et les administrations. Dans ce cas, même si l'on n'atteint pas l'universalité, l'extrême popularité d'un système, ou d'une norme, fait que la moindre atteinte un tant soit peu évoluée peut prendre des proportions énormes par effet d'échelle. Conficker dans ses différentes versions aurait infecté près de 7 millions d'ordinateurs, très souvent au sein d'entreprises ou d'organismes étatiques comme les ministères de la Défense des Etats-Unis, de France et du Royaume-Uni.

D'un autre côté des armes cyber très évoluées comme Stuxnet, même si elles sont destructrices, ne visent que des systèmes très particuliers. En l'occurrence le SCADA contrôlant des centrifugeuses à gaz de marque Siemens, cible unique de ce ver. Même s'il a fini par se répandre hors du centre de Natanz à cause d'une erreur humaine, son taux de viralité n'est pas comparable avec celui de Conficker ; 45 000 systèmes infectés au total contre 7 millions. Les autres agressions visant l'Iran et possédant les mêmes caractéristiques (ciblage précis et haut niveau de complexité) que sont Flame, DuQu ou Wiper ont abouti au même résultat : une agression forte et ciblée, touchant un nombre limité de systèmes. À l'inverse l'agression Aurora qui a visé Google, moins sophistiquée que Flame ou Gauss, a eu des effets très importants eu égard à sa cible. Des maliciels comme Gauss s'attaquent ainsi à des cibles très particulières limitées dans le temps ou dans l'espace – le système bancaire moyen-oriental dans ce cas – avec une dispersion très limitée, moins de 3000 ordinateurs dans le cas de Gauss.

En l'état il semble que le dilemme intrinsèque des cyberarmes soit le suivant : agir de manière ciblée en étant très puissant - dans le sabotage ou l'espionnage - ou agir de manière large mais avec des dommages limités.

121 Le risque de l'universalité des réseaux

L'universalité technique est avant tout celle de l'organisation des réseaux puisqu'il ne semble pas qu'elle puisse être atteinte au niveau logiciel, même si certains systèmes particulièrement populaires (Google, Microsoft) s'en approchent. Tout le projet américain dans l'affaire PRISM s'éclaire ici. En obtenant la collaboration des géants de l'Internet comme Google,

Facebook[69] ou Twitter, la NSA tentait de jouer sur l'effet de masse. Vu le nombre d'utilisateurs de ces derniers[70], une opération d'espionnage – ou plutôt une collaboration de renseignement dans le cas présent – est assurée de toucher un maximum de monde. Même si les actions de la NSA semblent être allées plus loin que ne le désiraient les sociétés impliquées, elles ont prêté un concours volontaire et généralisé à celui-ci. Le système de renseignement technique de la NSA[71] semble de moins en moins viser des cibles particulières suspectes et de plus en plus chercher à recueillir un maximum de données et métadonnées, pour les trier ensuite en quête de corrélations significatives.

Toutefois la limite de ce système de popularité est liée à la gratuité des outils comme Google ou Twitter. C'est cette dernière qui est à la base de leur succès – qui constitue d'ailleurs l'identité de Facebook dès la page d'accueil – mais elle pourrait aussi devenir leur principal handicap. Rien n'empêche les utilisateurs de se tourner du jour au lendemain massivement vers une nouvelle « norme » technique leur rendant des services équivalents s'ils estiment avoir été trompés par ces sociétés. La « marchandise » que traitent de telles sociétés - les données que nous leur fournissons notamment sur nous-mêmes - et dont elles vivent leur échapperait alors.

II Régulation juridique internationale

La régulation du cyberespace n'est pas que technique, elle a aussi l'ambition d'être juridique. Au fond, la question du droit du cyber est double. Il faut l'élaborer et l'appliquer, ce qui fait objet de débats, d'arguments et de positions plus ou moins instrumentalisées.

21 Régulation juridique du cyberespace

La régulation juridique du cyberespace est devenue un enjeu diplomatique. Elle se formule ainsi : comment assurer la sécurité et la stabilité du cyberespace ? Ceci a fait l'objet de

[69] Facebook revendique par exemple plus d'un milliard d'utilisateurs.
[70] En une minute il y a environ 700 000 requêtes Google.
[71] http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html ; consulté le 28/05/2014.

conférences internationales successives : la première à Londres à l'automne 2011, la deuxième à Budapest à l'automne 2012, puis à Séoul en 2013.

Deux positions antagonistes se dégagent :

- La première est qu'il faut élaborer un outil juridique contraignant, à destination des Etats, pour réguler – et donc stabiliser et sécuriser – Internet. Cette position est soutenue notamment par la Russie, la Chine ou l'Inde ;
- L'autre vise à maintenir le maximum de liberté d'Internet, jugeant que le droit international existant suffit et qu'il faudrait que les Etats et autres acteurs adoptent des principes de comportement et élaborent des mesures de confiance et une gouvernance en commun. Il s'agit de la position « occidentale » réunissant Etats-Unis, Europe et Japon.

Si l'on observe la position des grandes organisations internationales, le paysage est varié.

Lorsque la France en a assuré la présidence, le G8 a voulu développer des règles de comportement non contraignantes. Cela eut finalement peu de suites, car ce forum ne regroupe que huit pays, maintenant sept avec l'exclusion de la Russie.

Le Conseil de l'Europe a élaboré la Convention de Budapest contre la cybercriminalité (2001). Seuls 42 Etats l'ont ratifiée, Russie, Chine, mais aussi Espagne ou Suisse s'y sont refusés. Elle contient des mesures qui peuvent être efficaces mais souffre d'un défaut d'origine : elle a été proposée par le Conseil de l'Europe, donc par « l'Occident ».

Les Etats-Unis ont poussé pour que la cybersécurité soit prise en compte à l'OSCE, ce qui a conduit à un groupe de travail chargé de développer des mesures de confiance.

L'Assemblée générale de l'ONU a confié à des experts le soin de trouver une solution. La quatrième réunion d'un groupe de quinze experts gouvernementaux s'est tenue à l'été 2014.

Agence de l'ONU, l'Union Internationale des Télécoms a normalement une vocation technique, mais son rôle politique est finalement important. Le sujet de la cybersécurité y est régulièrement porté par la Russie, la Chine et d'autres dans l'idée d'y faire émerger des règles internationales ; à l'inverse les Etats-Unis veulent cantonner cette agence à un rôle technique.

L'échec du sommet de Dubaï a marqué l'impuissance du système onusien à réguler le cyberespace[72].

L'ICANN gère les noms de domaines (DNS) et l'attribution des adresses IP. Société de droit californien, dépendant du ministère du Commerce américain auquel elle est liée par un MoU[73]. Elle symbolise aux yeux de beaucoup la domination américaine. Elle a tiré parti de l'affaire PRISM pour réclamer son indépendance de droit. Ceci explique la décision des autorités américaines d'accéder à cette demande, du moins en apparence.

22 Discours juridique des principaux Etats sur la régulation du cyberespace[74]

Face à la construction de la menace cyber, certains Etats suivent un « réflexe » juridique, et tendent à invoquer le droit international afin de structurer voire de justifier leurs actions.

En 2007 l'Estonie, agressée, a cherché à invoquer l'article 5 du Traité de l'Atlantique Nord. L'OTAN n'a pas accepté cette demande, dans la mesure où les opérations en question tombaient visiblement en dessous du seuil de déclenchement du mécanisme de légitime défense collective, risquant de créer un précédent. Le discours des États au plan légal tend à se structurer autour de cette problématique: à partir de quel moment sommes-nous attaqués ? est-ce un acte de guerre ? et comment pouvons-nous légalement nous défendre ?

Si tous les Etats n'ont pas pris position sur cette question, elle a suscité une intense production doctrinale.

Le Professeur Michael N. Schmitt du Naval War College est l'un des pionniers de la doctrine juridique sur la cyberguerre[75]. Il est le juriste le plus prolifique sur la question (une dizaine d'articles traitant du *jus ad bellum* comme du *jus in bello*). Il a, de plus, supervisé la rédaction du Manuel de Tallinn. Michael Schmitt semble enfin avoir réuni au sein du *Naval War College* et de centres associés une ébauche d'école doctrinale autour de la problématique du droit de la cyberguerre (David E. Graham, Andrew C. Foltz, Matthew C. Waxman, notamment).

[72] Nicolas Mazzucchi, « Conférence de Dubaï : la régulation du net n'aura pas lieu » in *Sécurité Globale* n°24, 2013/2, pp. 41-47.
[73] Memorandum of Understanding.
[74] A partir d'une note d'étude juridique rédigée par Léa Tisserand, stagiaire à l'IRIS en 2014.
[75] Conférence du 22 juin 1999, *Naval War College Symposium, Computer Network Attack » and International Law.*

La question de l'influence de cette « école » sur la politique cyber du gouvernement américain est ouverte. Selon David E. Sanger[76], un groupe de juristes aurait assisté l'équipe technique qui a développé Stuxnet[77]. Lorsqu'on étudie la question de la légalité de ce virus sur la base des travaux de Schmitt, il resterait en-dessous des seuils d'application de la Charte des Nations unies[78]. La question de l'influence de Schmitt est sujette à caution.

S'agissant toujours des Etats-Unis, le général Keith Alexander a développé[79] un point de la doctrine juridique américaine sur la cyberguerre. En substance, une cyberagression est une agression armée. Cette doctrine, dans le milieu juridique, est appelée doctrine des dommages objectifs : on évalue l'attaque en fonction des dommages causés, sans tenir compte du vecteur de l'attaque. Les Etats-Unis se réservent donc le droit de recourir à la force physique dans le cadre de la légitime défense face à une cyberagression ainsi définie.

Pour les autres membres de l'OTAN, les prises de position et discours juridiques des gouvernements diffèrent passablement.

La France, dans les Livres blancs de 2008 et 2013, a posé les jalons d'une doctrine juridique plutôt axée sur la protection des opérateurs d'importance vitale pour la nation. Celle-ci fut actée par les articles 21 et 22 de la loi de programmation militaire pour les années 2014-2019 adoptée en décembre 2013. La France, à l'instar des Etats-Unis, se réserve une marge d'appréciation quant aux moyens à employer en cas de légitime défense militarisée, dont l'emploi de la force physique.

La doctrine dite des infrastructures vitales dispose d'une définition assez invariable selon les États[80]. Au risque d'une banalisation de la qualification d'agression armée[81].

---

[76] « One of the key planers told, much of it [les huits mois de travail nécessaires à l'élaboration de Stuxnet] [was] spent with lawyers trying to make sure that the code they were writing did not violate the laws of armed conflict »; in D. Sanger, *Confront and Conceal : Obama's Secret Wars and Surprising Use of American Power*, NYC, Crown, 2012, p.449

[77] Il semblerait aussi que des experts juridiques aient été consultés lorsque fut évoquée à Washington l'éventualité d'un frappe cyber contre la Syrie ou dans l'affaire ukrainienne. Ceci témoignerait d'un certain juridisme étatsunien, ou d'un souci de ne pas être accusés de crimes de guerre ou quelque chose de semblable. Dans tous les cas, les considérations sur les conséquences juridiques, médiatiques ou morales des armes informatiques offensives semblent singulièrement en freiner l'usage dans le pays sensé en être le mieux doté.

[78] Certains auteurs, proches de Schmitt, soutiennent le contraire, notamment : Andrew C. Foltz, « *Stuxnet, Schmitt Analysis, and the Cyber « Use of Force » Debate* », JFQ 67.

[79] U.S. Congress. Senate Committee on Armed Services. *Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command,* 15 avril 2010.

[80] Voir, pour une revue détaillée, Nils Melzer, Cyberwarfare and International Law, *UNIDIR Ressources*, 2011, pp.14-15.

[81] La position « finale » de l'article 51 dans la gradation des qualifications - menace contre la paix, rupture de la paix, agression et enfin agression armée, la différence entre les deux dernière étant particulièrement floue, mais liée à la gravité de la situation appréciée *in concreto.*

L'Allemagne, pour sa part, se réserve « le droit d'user d'armes conventionnelles en réaction à une cyberattaque sévère » dans le cadre de la légitime défense. Ce pays pencherait pour une interprétation particulière d'une cyberagression, évaluée par équivalence avec les dommages que causerait une attaque cinétique d'ampleur comparable.

Lors du dernier G8, la Russie a accepté la mise en place d'une ligne directe entre le gouvernement russe et le gouvernement américain, nouvelle version du téléphone rouge. En septembre 2000, le gouvernement russe a rendu publique sa doctrine de cyberdéfense (*Information Security Doctrine of the Russian Federation*) qui énumère les menaces contre la Fédération, dont une attaque contre les infrastructures critiques de l'État. Au plan international, les intérêts de la Fédération dans la « sphère informative » sont placés en exergue. Enfin, le développement de concept de la guerre de l'information par d'autres États est perçu par le Russie comme une menace externe. Au plan international, la Russie perçoit comme une menace grave la « propagande » étrangère et entend y remédier par voie législative en interne.

La Chine se positionne au plan juridique en réclamant l'extension du droit international existant au cyberespace, notamment sur la légitime défense et l'agression armée. Son point de vue sur la manière de définir une cyberagression n'est pas publié.

Dans ce contexte juridique et de ces débats sur la cyberagression, l'enjeu est celui du *seuil* et du *moment* du déclenchement d'une réponse militarisée de l'État ayant pris position. On peut aussi voir dans ce discours une forme de communication des Etats, mettant en avant une forme de ligne rouge à ne pas franchir sous peine de riposte.

Chapitre 5 - Cultures stratégiques

Parler de culture stratégique, c'est supposer que les invariants d'une culture - le mot étant pris au sens quasi ethnologique : ensemble des normes, croyances, acquis qui déterminent l'identité d'un groupe et se transmettent en son sein - se reflètent aussi dans sa pratique de la stratégie. Ceci inclut aussi l'attitude des membres de cette culture à l'égard de la discipline stratégique (par exemple, le fait que les lettrés chinois, et sans doute leurs modernes descendants, l'estiment hautement) et le patrimoine de textes sur l'art de vaincre[82]. On présuppose par là des paramètres correspondant à des styles nationaux et qui détermineraient la manière dont les citoyens ou les institutions tendent à considérer la conflictualité et les voies et moyens de la victoire.

I Ambiguïtés de la culture stratégique

Appliquée au cyber, la notion de culture stratégique comporte trois risques.

Le premier risque est de transposer en notre domaine des **stéréotypes** - l'Américain pragmatique et confiant dans la technique, le Chinois donnant du temps au temps pour parvenir à ses desseins, le Français individualiste et bricoleur, etc. - même si un stéréotype contient par définition une part de vérité.

La seconde difficulté est que, face à **l'universalité du numérique**, un monde que l'on se plaît à dire « sans frontières » ou « en mutation constante », il est tentant d'opposer technique à culture. Ce qui se diffuse partout de la même façon, l'usage de moyens numériques, ce qu'il suffit de recopier pour se l'approprier, la technique, semble peu conciliable avec les notions d'héritage, de variabilité d'un groupe à l'autre, de subjectivité et de pluralité des valeurs. Il est permis de douter qu'il y ait une façon bouddhiste ou chrétienne de concevoir un algorithme ou que des lectures de Sun Zi, Machiavel ou Clausewitz se reflètent vraiment dans le *modus operandi* de jeunes *hackers*.

De même, des entités géopolitiques pourraient bien répondre par les mêmes moyens aux mêmes pressions, et, suivre un mouvement général, sans que cela reflète une culture proprement chinoise, iranienne, etc.

[82] Voir Biehl Heiko, Giegerich Bastian & Jonas Alexandra (Eds.), *Strategic cultures in Europe*, Springer, 2013, VI, 401 p.

Ainsi, il est fort probable qu'un pays autoritaire va :

- renforcer en priorité ses capacités défensives face à un monde qu'il croit a priori hostile ;
- renforcer ses capacités de surveillance, de traçage et d'infiltration de l'opposition avec de nouveaux outils numériques ;
- se doter de moyens offensifs à la fois contre les objectifs militaires et contre les infrastructures d'autres pays ;
- se pourvoir autant qu'il le pourra de technologies nationales et de matériel sécurisé, pour s'assurer qu'aucune puissance étrangère ne peut l'espionner via le matériel ou les logiciels qu'il utilise ;
- tendre à se protéger des « influences idéologiques externes » (quitte à les qualifier « d'offensives subversives, séparatistes, antinationales, de discours de haine », etc.) et à rechercher les outils techniques et juridiques ou les alliés qui l'y aideront[83].

Ce schéma s'applique sans doute à la Chine, à l'Iran et à d'autres : ce sont des réponses logiques, fussent-elles immorales, à des besoins similaires.

Le troisième problème est que nous ne connaissons souvent la stratégie d'un pays que par ses écrits théoriques et discours officiels. Or ceux-ci peuvent être destinés à tromper ou rassurer. Ou alors ce sont ses adversaires qui définissent le *modus operandi* et la mentalité d'un pays en matière de cyberstratégie ; ainsi, les études américaines sur les agressions supposées venir de Chine.

Il nous semble pourtant qu'il existe à l'échelon régional, ou national, des différences d'emploi des mêmes outils et des divergences dans la manière de concevoir les objectifs généraux et des moyens d'y parvenir dans le cyberespace.

Pour le dire autrement, il serait paradoxal que l'idéologie, les traditions nationales, la représentation générale que l'on se fait des autres pays et de ses intérêts, les façons de concevoir le temps, les relations entre individu et collectif, l'économique et le politique, et autres éléments culturels ne se reflètent pas dans sa cyberstratégie. Même si c'est en

[83] Les stratégies des pays autoritaires sont régulièrement analysées par l'ONG Reporters Sans Frontières, dans un un rapport annuel sur les « ennemis d'Internet » disponible sur leur site http://fr.rsf.org

concurrence avec des facteurs plus objectifs, comme le PIB, l'état d'avancement technologique ou la position géographique, des catégories intellectuelles se reflètent forcément dans la manière de concevoir et mener des opérations cyber. Nous convenons donc de nommer ce déterminant « culture stratégique ».

II Quelques exemples de culture stratégique

21 Le cas français

Quelle grille appliquer à la France, par exemple ? En reprenant le « pacte défense cyber » officialisé en 2014[84] ou des textes comparables il n'est pas rare de retrouver des constantes qui semblent témoigner d'une vision nationale. Celle-ci comprennent la protection de la souveraineté, l'indépendance, la dissuasion du faible au fort, le goût de grands projets industriels, les notions de rayonnement de l'armée et de lien armée/nation, une certaine tradition de l'ingénieur, un culte de l'excellence, et autres idées chères aux élites républicaines.

La protection des infrastructures vitales avec ce que cela implique en termes de technologie, de recherche, de formation, de sensibilisation, d'anticipation tient une grande place dans le pacte, ce qui n'a, certes, rien de spécifiquement français. Mais les spécificités nationales se retrouvent dans la notion d'une posture globale de sécurité et dans le projet d'une industrie nationale et européenne de la cybersécurité, thèmes qui reviennent comme des *leitmotive*. L'implication du secteur privé, celle du citoyen, notamment le cyberréserviste, semblent aussi conformes à une tradition intellectuelle qui exalte le dévouement pour le bien commun et le pacte républicain. Faire lien, faire communauté, se dévouer, exceller, rayonner, se rassembler pour la nation : de telles notions nous viennent assez naturellement, ce qui pourrait bien être l'indice qu'elles sont en réalité culturelles. La contribution à la défense des frontières, fussent-elles « numériques » et ne coïncidant pas exactement avec le sol sacré de la patrie, justifie la volonté française de se doter d'armes informatiques offensives. La notion même d'une arme dissuasive « nationale », version cybernétique de la force de frappe, correspond à une tradition nationale. Sans être absolument déterminante - il n'y a rien dans le pacte, par exemple, qu'un autre pays européen ne puisse transposer chez lui sans contradiction majeure

[84] Le texte est téléchargeable sur le site http://defense.gouv.fr

– la notion de culture stratégique nationale pourrait expliquer une prédisposition à faire certains choix.

22 Le cas chinois

Le cas qui appelle le plus de commentaires en termes de cultures et mentalités est celui de la Chine. Ceci à la fois parce que l'on ne prête qu'aux riches et parce que nous sommes habitués à opposer un Occident clausewitzien, qui pense « cause et effet » ou « force contre force » à une Chine toute imprégnée de la subtile logique de Sun Zi. La difficulté d'accés à des textes actuels de doctrine chinoise renforce cette tendance à se référer à des constantes. La principale exception, le traité sur *La guerre hors limites*[85], traduit dès les années 1990, a nourri l'idée d'une vision chinoise dans laquelle la pluralité des moyens de vaincre - le cyber est brièvement évoqué parmi d'autres - est pensée de façon quasi symphonique, comme participant de grands équilibres, et où l'action du stratège consiste à penser très en amont les conditions d'une évolution générale des rapports de force[86].

Si l'on synthétise les traits réputés constants de la stratégie chinoise, la liste comportera généralement :

- la vision sinocentrée d'un Empire entouré de peuples dont il doit se protéger, mais dont il peut attendre des contributions. Ainsi, leur emprunter leurs meilleures techniques et prenant garde de ne pas menacer l'identité chinoise ;
- une tendance à penser la manœuvre stratégique à long terme, en préparant très en amont les conditions matérielles et psychologiques de la victoire ;
- une prédilection pour la ruse ou les stratagèmes, le goût d'une action souvent indirecte, calculée en fonction des réactions des adversaires et les prédispositions des autres acteurs ;
- la manœuvre asymétrique privilégiant les rapports entre des principes opposés dont il faut doser les usages.

En suivant ce schéma on attribuerait :

[85] Q. Liang et W. Xiangsui, *La guerre hors limites*, Paris, Bibliothèque Rivages, Payot&Rivages, 2003.
[86] Une notion, correspondant à l'idéogramme « che », faire advenir ce qui est en puissance, que François Jullien présente comme fondamentale dans la mentalité chinoise : voir *La propension des choses*, Seuil, 1992.

- à la première tendance, le projet d'une « grande muraille de feu » protégeant des influences numériques extérieures et permettant de surveiller les internautes chinois, tout en considérant qu'il est légitime de s'emparer des connaissances des étrangers via l'espionnage informatique ;
- à la seconde, la création, dès les débuts de l'introduction d'Internet en Chine, de technologies, plateformes, fournisseurs d'accès nationaux, donc susceptibles d'être contrôlés par l'État central ;
- à la troisième, le dessein de prélever un maximum de données ou de préparer de futurs moyens d'agression, par une pénétration systématique occulte des dispositifs informatiques d'autres pays, de compagnies étrangères ;
- au quatrième, le choix du cyber, intégré dans une panoplie stratégique plus vaste, envisagé comme un moyen privilégié d'acquérir de la puissance et de modifier à faible coût des équilibres et déséquilibres généraux.

Une des caractéristiques des offensives chinoises (le lecteur comprendra : « attribuées à la Chine ou à des acteurs dont les adresses IP sont en Chine ») est de procéder par campagnes massives et par vagues. Certaines ont reçu des noms : Byzantine Candor (commencée peut-être en 2002), Titan Rain (sans doute commencée en 2003) Shady Rat (lancée à partir de 2006), Ghostnet (découverte en 2009), Aurora (découverte en 2010). Elles sont classées le plus souvent comme des *Advanced Persistent Threats*[87]. En pratique, ces agressions se développant à partir d'un point d'entrée, visant à prendre le contrôle d'un système important sur une longue durée, et à y prélever des données sans être détectées, le tout en fonction d'objectifs politiques ou économiques à l'échelle d'une nation. La méthode consisterait donc à pousser systématiquement ses pions, à multiplier les agressions, pas forcément les plus sophistiquées, mais de grande ampleur, avec un personnel considérable et de manière assez bureaucratique. Tel est, du moins, le portrait qu'en dressent des rapports comme celui de Fire Eye sur les Menaces Persistantes Avancées, terme qui semble systématiquement accolé aux pratiques chinoises.

Dans la liste des victimes du « cyberdragon », se retrouvent aussi bien des infrastructures critiques (énergie, gazoducs, digues, Departement of Homeland Security) que des grandes

[87] Menaces avancées persistantes, même si la définition exacte de ce terme n'est pas très bien fixée.

sociétés comme Google, Adobe, Lockheed-Martin, Northrop-Grumman, des médias, services financiers comme Morgan Stanley ou la chambre américaine de commerce.

Le cyberespionnage chinois, outre les Etats-Unis, s'en prendrait aussi à la chambre des communes britannique (2006), à des intérêts allemands (2009), à l'Inde, à la Corée du Sud, au Japon, à des pays de l'ASEAN (Laos, Malaisie, Philippines, Singapour, Vietnam, etc.), presque toujours dans une perspective d'espionnage.

La « patte » chinoise se reconnaîtrait à l'ampleur des agressions ou des forces mobilisées - voir Ghosnet serait actif dans une centaine de pays - plutôt qu'à une sophistication extrême. Ces actions recourraient à des modes de compromission assez simples, par hameçonnage ou par l'envoi d'un document infecté joint à un mail, avant exploitation systématique des failles découvertes.

Quant au choix des cibles, il mêle souvent des institutions publiques, voire militaires et des centres de recherche, ONG, *think tanks*, entreprises de pointe. S'y ajoutent parfois des cibles plus ouvertement « idéologiques » comme de supposés activistes tibétains et ouïgours.

En France aussi, le cyber-espionnage chinois est souvent évoqué : on lui a un moment attribué le pillage des ordinateurs de Bercy en 2011, sans oublier les soupçons portés par le rapport du sénateur Bockel contre le matériel de routage *made in China*. Le 26 octobre 2013, Israël déclarait avoir déjoué une agression chinoise contre 140 industries de défense et de sécurité par un pourriel porteur d'un cheval de Troie. Bref, il semblerait que le spectre du hacker chinois hante le monde

Aux Etats-Unis les rapports successifs pointent la responsabilité de Pékin avec une grande constance. Dès 1999 le département de l'Énergie se préoccupe d'une pénétration chinoise susceptible de menacer la sécurité nucléaire du pays. Dix ans plus tard, en 2009, un rapport de Northrop-Grunman analyse « les capacités de la République populaire de Chine pour conduire la cyberguerre et l'exploitation de réseaux d'ordinateurs » et prédit pour un proche avenir des intrusions dans les systèmes d'information, occidentaux en particulier, à des fins de renseignement. Le niveau des agressions excède les capacités de simples particuliers ou d'organisations privées et, dans un pays aussi surveillé, des pirates ne pourraient subsister sans au moins l'accord tacite du gouvernement : tels sont les arguments qui servent à impliquer Pékin dans toutes ces affaires.

L'Armée Populaire de Libération engagée dans le cyber et y mettant les moyens, disposant d'une doctrine (*La guerre hors limites*, op. cit.), de capacités offensives, avec une stratégie d'infiltration et d'espionnage très en amont et éventuellement complétée par le recours à des mercenaires ou à des pirates informatiques, ce tableau a un corollaire : la Chine est souvent désignée outre-Atlantique comme l'ennemi principal.

Le rapport Mandiant de 2013 synthétisant six ans d'enquête, désigne même l'unité 61398, dite aussi Comment Crew, dépendant de l'Armée Populaire de Libération, dans la banlieue de Shanghai. Cette équipe d'élite aurait prélevé des quantités remarquables de données sensibles chez une centaine de clients de Mandiant, allant de Coca Cola aux opérateurs d'infrastructures vitales dont la distribution de l'électricité.

De la même façon, un rapport de la société Kaspersky identifie peu après une autre unité de hackers chinois qu'il nomme Red Star APT : une cinquantaine de personnes actives depuis 2005, et qui auraient visé aussi bien des activistes tibétains que des institutions diplomatiques ou universitaires, des fournisseurs de la défense, des sociétés pétrolières.

La rencontre entre B. Obama et Xi Jinping en Juin 2013 a été l'occasion de rappeler les griefs des Etats-Unis mais la Chine se plaint de son côté d'être la première cible au monde en nombre de cyberagressions[88].

23 Le cas russe

La culture stratégique chinoise appelle une comparaison avec la culture russe, tant nous sommes habitués à rapprocher ces deux rivaux principaux des Etats-Unis. Tout ce qui touche la cyberstratégie russe est entouré d'un certain mystère, hors le sabotage cyber en parallèle à l'offensive cinétique contre la Géorgie en 2008, cas où nul ne doute de la responsabilité des troupes russes.

Dans le cas de l'Estonie l'année précédente, l'opération – au final un grand déni d'accès - a envoyé un message clair sur ce qui se produit lorsqu'un pays de l'ex-URSS touche à un intérêt symbolique russe. En revanche, ni l'impact réel de ce qui fut en son temps présenté

[88] À noter que les autorités chinoises qui ont toujours nié être à l'origine des attaques qui leur sont attribuées et que, lorsqu'un grand jury américain a inculpé cinq militaires chinois pour cyberespionnage en mai 2014, l'Académie chinoise du cyberespace a riposté en accusant les Etats-Unis de mener un cyberespionnage bien plus ample et « sans scrupule » à leur égard (« La Chine accuse à son tour les Etats-Unis de cyberespionnage, dépêche Reuters du 26 mai 2014).

comme la « vraie première cyberguerre » et l'identité exacte des agresseurs - services d'État russes, groupe de hackers patriotes Nashi, éventuellement cybermafia – ne sont pas si évidents.

L'affaire Octobre rouge découverte en 2012 par la firme Kapsersky est plus complexe encore : il s'agit d'un logiciel espion actif cinq ans visant des centres de recherches et entreprises stratégiques pour y voler des données. Celles-ci étaient-elles revendues par des acteurs privés (dont certains auraient été russophones), à un État commanditaire ? S'agirait-il, comme ce fut dit, de l'exploitation d'une faille découverte initialement par des pirates chinois ? Que faut-il déduire du fait que nombre de cibles étaient situées sur le territoire de l'ex-URSS ? D'autres accusations portant sur des intrusions dans le système de l'US CENTCOM ou sur le Climategate circulent aussi et pointent vers la Russie.

Nombre de commentateurs prêtent une certaine sophistication aux agressions russes ou présumées telles, ainsi qu'un grand sens de la dissimulation dont témoignerait l'usage de faux drapeaux.

Avec toutes les réserves nécessaires, le tableau qui se dessine est celui d'un pays où les structures souveraines (services de renseignement, ministère de la Défense, de l'Intérieur et de la Justice) mènent ou commanditent des actions d'espionnage complexes et utilisent l'arme cyber de façon plus brutale ou offensive dans l'ancienne zone d'influence soviétique. Toutes choses correspondent à l'image la plus répandue des héritiers de l'URSS. Des textes américains décrivent des alliances entre services d'État russes, fidèles à une tradition de contrôle idéologique de la population et de prééminence des services secrets, et, d'autre part, des intérêts privés, voire des groupes mafieux, qui agiraient à la façon de cybermercenaires comme le groupe Runet. Cette même littérature oppose le « péril chinois » massif et visible au péril russe plus discret mais de meilleur niveau technique et intégré à une vision stratégique globale.

Par ailleurs, si l'on se tourne vers les sources russes, notamment vers des textes doctrinaux comme « Considérations conceptuelles sur les activités des forces armées de la Fédération russe dans l'espace informationnel »[89], d'autres particularités transparaissent. À commencer par une question de vocabulaire : les stratégistes russes parlent d'un « espace informationnel »

[89] Voir sa présentation par Yannick Harrel dans Sécurité Globale, dossier « *Cyber : la guerre a commencé* /1 » (213/1 n° 23), pp. 65-71.

où il s'agirait d'assurer la sécurité militaro-politique et de coopération avec les pays du Traité de Sécurité Collective (OTSC), de l'Organisation de Coopération de Shanghai (OCS). Dans cette vision la différence entre une agression purement informatique (de type paralysie des infrastructures vitales) et une agression informationnelle, voire une action de propagande, devient secondaire.

Les références à des normes internationales qui respecteraient les souverainetés nationales (position commune à la Russie et à la Chine lors de la rencontre de Dubaï) ainsi que la nécessité d'éviter l'escalade, dans le cyberespace aussi, ne sont pas sans rappeler un certain discours soviétique sur la dissuasion. À l'époque, il s'agissait autant de gagner en légitimité internationale et en soutiens idéologiques à travers le monde que de se protéger contre des influences idéologiques extérieures. Dans cette continuité, les conflits du cyberespace sont pensés en termes de légitime défense, de souveraineté à protéger et d'opérations informationnelles offensives. Ces dernières peuvent aussi bien relever de la subversion par l'information ou d'une version modernisée de la guerre psychologique que de la pure ingénierie informatique. Dans tous les cas, la culture russe du cyber semble privilégier la couche logique ou sémantique.

24 Le cas israélien

La question des cultures stratégiques se pose à propos des conflits qui déchirent le Moyen-Orient et le monde islamique, même en mettant de côté le cyberjihad[90].

Israël joue un rôle à part, comme cible préférentielle d'un certain nombre de pays ou d'organisations de la zone, mais aussi du fait de sa réputation d'excellence en matière d'informatique, de hacking ou de cyberopérations. Ainsi, un moment la thèse attribuant la paternité de Stuxnet aux seuls services israéliens a circulé, sans que cela n'étonne personne. « Quand vous pensez cyber, pensez Israël » déclare Benjamin Nethanyaou à la *cyber tech conférence* de Tel-Aviv en janvier 2014. Même s'il est permis de soupçonner un élément « publicitaire » voire une communication de dissuasion dans cette façon de vanter la qualité de ses unités cyber, les efforts investis par Israël dans ce domaine sont incontestables et

[90] Personne ne nie que les groupes se référant à al Qaïda n'utilisent beaucoup le cyberespace via des réseaux sociaux pour le recrutement, l'expression à l'égard du monde extérieur et la messagerie interne ; l'existence de véritables cyberagressions inspirées par des groupes jihadistes est âprement discutée. Pour notre part, en dépit d'annonces terrifiantes répétées depuis 2001, nous n'avons guère constaté d'attentat par écran interposé qui ait fait des dégâts terrifiants.

s'appuient sur l'exploitation du potentiel des jeunes hackers, dans un pays où ils ne sont pas rares.

La participation de tous les citoyens à la défense est mise en valeur par un État qui se sent menacé de toutes parts et entend défendre ses infrastructures[91]. Si Israël a subi force agressions informatiques, pas forcément de très haut niveau, reste qu'il investit beaucoup, financièrement et techniquement, dans une protection tous azimuts. Cette défense numérique du territoire va de pair avec la recherche de capacités offensives et de renseignement cyber, y compris pour empêcher la « croissance des capacités militaires des ennemis d'Israël » comme l'affirme *IDF in cyberspace : Intelligence Gathering and Clandestine Operations*[92] par Rotem Peso sur le site de Tsahal. La dissuasion s'appuie sur la qualité technologique, la modernité, la combativité et la solide expérience dans le domaine du renseignement dont se prévalent les Israéliens ; tout cela finit par ressembler à une culture stratégique de mobilisation permanente qui transposerait dans le cyberespace les constantes de la culture militaro-politique du pays.

25 Les cas iranien et syrien

Peut-on trouver des caractéristiques aussi marquées dans le camp adverse et dont témoigneraient les cyberagressions menées contre Israël ?

Il faut procéder par hypothèses. Ainsi le virus Mahdi, découvert par Kaspersky en 2012, aurait infecté à des fins d'espionnage des ordinateurs bien ciblés en Iran, en Israël, et en Afghanistan pour les zones principales. Or le nom de Mahdi renvoie à la figure mystique du rédempteur qui gouvernera la terre avant le Jugement dans l'eschatologie des chiites duodécimains. De même, dans l'opération Shamoon que beaucoup soupçonnent d'avoir été commanditée par Téhéran, la démonstration de cette implication repose sur l'hypothèse que les acteurs affichés ne seraient qu'un complice voire un paravent de l'Iran.

L'Iran lui-même, cible de Stuxnet et des ses dérivés (DuQu, Flame, Gauss, etc.) dit construire une cyberstratégie, reposant un contrôle des contenus, vouloir créer un « Internet halal » à l'abri des influences étrangères, une défense contre d'éventuelles agressions cyber et de se doter de capacités d'attaque ou de rétorsion.

[91] Comme le sabotage mené contre la régulation du tunnel routier du Mont Carmel menant à Haïfa (8 septembre 2013).
[92] Voir http://www.idf.il/1283-16122-en/Dover.aspx, consulté le 7 mai 2014.

Quant à la Syrie, elle offre un autre exemple d'un pouvoir autoritaire capable de s'adapter aux nouvelles technologies. En témoignent la façon dont Damas a su moduler l'usage des instruments de contrôle et le filtrage du Net et surtout utiliser l'AES.

Ces faits, comme la réputation du Hezbollah en matière cyber, semblent indiquer une prédisposition des États ou mouvements activistes proches de l'Iran à explorer de nouvelles voies stratégiques y compris dans le cyberespace, mais rien de plus pour le moment.

26 Le cas américain

La culture stratégique américaine pose un problème inverse : la surabondance de publications et de sigles, concepts, principes, ou autres. L'évolution des doctrines successives (comme ce fut le cas pour la dissuasion atomique), la capacité de ce pays d'inspirer par son *softpower* les pays alliés et notamment leur façon d'envisager la cyberstratégie, mais aussi les jeux de pouvoir entre administrations et la vigueur des débats outre-Atlantique : de tout cela naît une complexité aussi troublante que le manque d'indices pour d'autres pays. Ici la question est moins de savoir ce qu'il y a de « culturel » ou de spécifique dans la vision américaine du cyberespace, que de distinguer des constantes face à la prolifération des textes.

On tentera pourtant de suivre quelques pistes.

L'angoisse de la force

Le thème est ici celui des infrastructures vitales menacées et du « grand accident » ou de la grande agression. Le « Big One », le Pearl Harbour informatique - d'autres préfèrent parler de Cybergeddon, l'Armageddon cybernétique - revient depuis longtemps, comme l'attente d'un danger quasi existentiel, rançon à payer pour l'hyperpuissance. Le pays le plus avancé dans le domaine informatique semble éprouver une peur à mesure de sa dépendance à l'égard de ses outils et réseaux informatiques. L'obsession de voir sa force (l'ouverture sur les réseaux, l'incarnation d'un modèle mondial de la société de communication *high tech*), se transformer en faiblesse n'est donc pas neuve[93]. Dès les années 1990, une abondante littérature stratégique, relayé par les œuvres de fiction, évoque le fantasme d'un écroulement du système par contagion : la solidarité des infrastructures vitales qui dépendent d'un contrôle informatique les rend vulnérables à une propagation en chaîne du chaos. Cette peur inspire les déclarations

[93] En France, elle était déjà analysée en 2001, notamment dans Panoramiques n°57 « L'information, c'est la guerre » et dans *L'ennemi à l'ère numérique* de F.B. Huyghe (P.U.F.).

récurrentes sur une cyberguerre ou guerre de l'information que les Etats-Unis perdraient du fait de leur ouverture au monde ou de leur surexposition[94].

L'Autre comme ennemi

Ce thème recoupe souvent avec celui de l'ennemi extérieur qui prendrait la suite de l'URSS : suivant les cas, Chine, Fédération de Russie ou des adversaires « terroristes », asymétriques, proliférants puisque les cyberarmes sont assimilées à des armes de destruction massive. Nombre de stratégistes voient donc les Etats-Unis comme la cible par excellence de « ceux qui haïssent la liberté ». À d'autres périodes, la cybermenace iranienne remonte dans le palmarès des dangers, mais le principe reste le même : la cyberdéfense des Etats-Unis, la « nation exceptionnelle » confrontée aux agressions venues du reste du monde (*ROW* : *Rest Of The World*). En nommant l'agresseur en puissance, stratégiquement redoutable parce que moralement coupable, les milieux stratégiques américains un choix qui n'est pas celui de tous les pays occidentaux. De même, le rapprochement entre cyberagression et acte terroriste est récurrent : l'ennemi terroriste/cyber prépare dans l'ombre une agression par surprise profitant des vulnérabilités d'une société « ouverte » pour frapper au cœur.

Le cyber comme espace de la guerre

Décrivant depuis plusieurs décennies une cyberguerre (Estonie 2007, Géorgie 2008, Shamoon 2012, qui sont autant de prétextes successifs pour proclamer que « cette fois, la vraie cyberguerre a commencé »), la littérature étatsunienne sur le sujet[95] se réfère souvent aux catégories guerrières - comme l'agression armée, le droit à la riposte ou à la rétorsion, la guerre juste, l'acte de guerre, etc - transposées à des situations de cyberconflictualité. Le droit de riposte dans la doctrine américaine, riposte qui combinerait réponse cyber et réponse cinétique pour châtier les agresseurs, témoigne bien de cette militarisation du cyberespace assumée sans complexe et justifiée en droit et en morale.

La cyberdissuasion tient une place qu'il est facile d'expliquer par l'héritage de la guerre froide. Là encore, sa critique, menée par exemple par Martin Libicki dans les publications de

[94] Le thème de la cyberguerre que perdraient les américains revient depuis plusieurs années. Voir par exemple les prises de position de Jeffrey Carr dès Juillet 2011 (http://jeffreycarr.blogspot.fr/2011/07/why-us-will-lose-war-in-cyberspace.html, consulté le 28 mai 2014).

[95] Les sceptiques qui considèrent la cyberguerre comme un *hype*, une exagération, ne manquent pas non plus, un des plus célèbres étant Thomas Rid (p.e ; « Cyberwar and Peace » in Foreign Affairs, numéro de novembre-décembre 2013, disponible sur http://foreignaffairs.com consulté le 28 mai 2014.

la Rand[96], n'est pas négligeable mais le seul fait de débattre en termes de dissuasion ou de moyens de rétorsion rendant l'agression « trop coûteuse » pour que l'autre songe à l'entreprendre, tout cela reflète une vision à la fois globale et dramatique du péril cyber.

L'omnisurveillance

Enfin, on ne peut oublier le rôle de la surveillance dans le dispositif de sécurité. Les révélations sur le système de la NSA par E. Snowden ont suscité force références à *Big Brother*, voire au panoptique (*Panopticon*) de Bentham popularisé par Foucault[97]. En dépit de leur intérêt littéraire, ces citations nous paraissent occulter l'essentiel. Outre que les Etats-Unis restent un pays où la défense du citoyen contre tout excès étatique reste très vigoureuse, le système NSA diffère d'une surveillance de type totalitaire. Cette dernière est fondée sur la crainte du citoyen : les prisonniers décrits par Bentham ou Winston, le héros d'Orwell, savent qu'ils sont constamment observés dans un univers clos où rien n'échappe au surveillant et où toute déviation est punie. Le but est d'enregistrer les fautes et de susciter une autodiscipline alimentée par la crainte qu'éprouve chacun de se trahir et d'être pris. La surveillance exercée par la NSA est d'une autre nature, pas seulement parce qu'elle est, ou plutôt était, clandestine. Ceux que repère la grande agence ont rarement à craindre une arrestation à l'heure du laitier. En revanche, les ambitions étatsuniennes dans le domaine de l'anticipation des comportements sont déterminantes.

Le système NSA reflète certes les craintes de l'après 11 septembre et l'enchaînement de mesures préventives liberticides qu'incarne le Patriot Act, mais il s'inscrit aussi dans une histoire plus longue, notamment celle du pacte dit UK-USA et du système Echelon. Trois réponses technologiques comparables sont nées pour répondre à trois besoins successifs : surveiller l'ennemi soviétique, s'assurer la prééminence technologique dans la période qui suit la chute du Mur et mener une lutte contre le terrorisme après 2001. Sur une période de plusieurs décennies, se retrouvent, outre l'inévitable « technophilie »[98] et l'attraction pour les instruments de communication et de calcul, une ambition de tout savoir pour se prévenir de tous les dangers et, idéalement, empêcher les « crimes » juste à temps.

[96] Les publications de ce chercheur sont disponibles sur le site de ce think tank : http://rand.org.
[97] Notamment dans *Surveiller et punir*, Gallimard, 1975.
[98] La technophilie se caractérise par un enthousiasme pour les technologies, en particulier de la communication. À noter le lancement d'une notion proche celle de « solutionionisme » par Eugeny Morozov, qu'explique le titre de son dernier livre « « To Save Everything,Click Here : The Foly of Technological Solutionism », Philadelphie, Public Affairs, 2014.

L'ancienne surveillance est tournée vers le constat des fautes ou la détection des "complots" à partir des messages des comploteurs, donc vers l'interception ciblée de contenus. À cela, se substitue une entreprise tournée vers la prédiction et les grands nombres. En combinant la « pêche au chalut » de milliards de données et surtout de métadonnées (*upstream* sur les câbles sous-marins d'Internet, *downstream* chez les fournisseurs d'accès et opérateurs), plus des méthodes de hackers, plus l'espionnage de dirigeants « à l'ancienne », plus des actions ciblées sur la couche matérielle et logicielle..., la NSA mène une collecte qui se chiffre en milliards de données et pétabytes. L'utopie de la *total information awareness* et de la prédiction totale non par traitement d'échantillons représentatifs, mais par mise en corrélation d'une masse de données révélatrices sur chacun semblent être une constante de la stratégie américaine dans le cyberespace.

Influence et soft power

Cette volonté d'anticipation totale correspond à une vision tout aussi globale de la cyberdéfense. Le *cyberpower,* concept proposé par Joseph Nye pour compléter ceux de *soft* puis *smart power,* inclut des composantes politiques - comme la volonté d'assurer la présence des Etats-Unis partout sur la Toile -, mais aussi une cyberdiplomatie, une forte présence sur les réseaux sociaux ou la nécessité de s'identifier aux yeux du monde avec la cause d'un Internet libre et sécurisé. La présence du département de la Défense, qui tend à penser le cyberespace comme cinquième espace de bataille où s'étendrait naturellement sa prééminence est forte, comme l'est la volonté économique et technologique de se doter des technologies les plus sûres et des systèmes d'alerte les plus sophistiqués... Le tout forme un mélange de *soft power* (l'attractivité et l'exemplarité des Etats-Unis qui doivent incarner le modèle mondial de la future société de l'information) et de volonté de sécurité tous azimuts.

Difficile de résumer ces conceptions autrement que par « tout[99] » : tout craindre, tout contrôler, tout prévoir, tout sécuriser, pouvoir tout atteindre, etc. Cela équivaut à un principe d'exclusion : n'admettre ni aléa, ni risque, ni compétition, ni menace potentielle dans le domaine du cyberespace considéré comme celui de l'expansion naturelle d'une Amérique dont la cause s'identifie à celle de l'universel et dont les intérêts coïncident avec une gouvernance associant États, société civile et secteur privé.

[99] Allusion au projet dit *Total Information Awareness* de l'amiral Pointdexter, un programme de l'US Information Awareness, lancé en 2003 et destiné à combattre le terrorisme par une gigantesque collecte de données.

Tous ces facteurs culturels ou représentatifs d'une certaine mentalité pourraient bien se retrouver dans le premier choix stratégique qui s'offre à l'acteur : celui du type d'agression.

Chapitre 6 - Les choix du type d'agression

Pourquoi attaquer ? Quel type d'agression choisir dans le cyberespace ? Comme les offensives ne sont plus accompagnées de ces proclamations qui marquèrent longtemps le passage du rapport de deux États, allant du différend à l'hostilité armée, il faut raisonner de façon hypothétique. Donc se placer du point de vue de l'agresseur, reconstituer sa démarche intellectuelle au regard de ses buts.

Des dizaines de théories traitent de l'origine - pulsionnelle, rationnelle et intéressée, culturelle, structurelle. - des mécanismes de la violence, de ses cibles individuelles ou collectives, de la spécificité de la guerre[100]. Difficile d'en privilégier une - psychanalytique ou sociologique par exemple - pour faire la polémologie d'agressions par écrans interposés et qui ne semblent obéir qu'à de purs calculs rationnels.

Entre l'obscurité qui entoure ses motivations et la dimension technique et instrumentale de sa réalisation, la cyberagression défie les modes de raisonnement traditionnels.

Faisons pourtant l'hypothèse que le plus moderne peut s'éclairer par le plus ancien et que les catégories classiques de la philosophie politique peuvent s'appliquer quitte à ce que soit *a contrario.*

Si le cybermonde est en puissance le théâtre d'une guerre de tous contre tous, pourquoi ne pas remonter aux catégories fondatrices proposées par l'auteur du *Léviathan* (1651) ? Selon Hobbes, qui reprend une idée chère à Thucydide, dans un état de nature, les acteurs combattent par besoin de compétition en vue du gain, par méfiance liée au besoin de sécurité et par recherche de la « gloire » ou quête de la réputation. Ces catégories ne s'appliquent pas forcément à un stade historique, mais servent plutôt de fiction utile et de point de référence théorique. Et personne ne pense que les comportements des États ou des acteurs organisés soient forcément réductibles à celui des individus avant le contrat social. Risquons pourtant le paradoxe : la grille du XVII^{e} siècle pour éclairer nos conflits du XXI^{e}.

A priori, les agressions pour s'emparer de données précieuses correspondent à l'appétit de richesses. Les manœuvres contre les systèmes d'information adverses au projet d'affaiblir un

[100] Sur la transposition de ces catégories au monde cyber voir François-Bernard Huyghe, *L'ennemi à l'ère numérique* PUF, 2001, où nous parlions de « quatre arts martiaux » permettant de lutter dans le monde numérique : apparaître, tromper, savoir, cacher, ce qui, si l'on considère « cacher » comme l'art défensif de préserver ses secrets, est parfaitement conciliable avec les catégories employées ici.

rival dangereux pour assurer sa propre sécurité. Quant à la subversion, avec toutes nuances de l'humiliation, de la provocation de la dénonciation, qu'elle peut recouvrir, elle évoque bien le besoin de reconnaissance ou de réputation.

Sans tomber dans le réductionnisme - trois passions éternelles de l'homme fonderaient trois types d'agressions hautement techniques et stratégiques -, la trilogie hobbesienne mérite au moins l'examen.

I L'espionnage : quel gain ?

1.1 Espionner pour se procurer un avantage

Les agressions relevant de l'espionnage servent à s'emparer d'une information-richesse en la dérobant à son légitime propriétaire. Il circule des chiffres difficiles à vérifier, mais qui s'élèvent toujours à des milliards de dollars, sur les pertes que subiraient ainsi des économies. Espionner est un moyen au service du projet immoral mais rationnel d'améliorer sa compétitivité, de gagner des marchés, de se doter d'outils de développement aux frais d'autrui. L'espionnage informatique,par définition caché, souvent durable tant que la fuite n'a pas été découverte, permet de gagner du temps sur un concurrent : temps de retard en recherche et d'investissement que l'on comble ainsi ou temps d'avance que l'on gagne en se procurant maintenant ce que l'on aurait sans doute fini par savoir, mais trop tard; après que le concurrent ait exploité son avantage informationnel.

L'espionnage sert donc à se procurer un avantage indu. La plupart des accusations portées contre la Chine relèvent de ce mécanisme pratiqué à grande échelle. Une grande part des cyberagressions constatées visent tout simplement au viol de la confidentialité. Le cyberespionnage ne demande pas forcément une recherche de pointe et peut se pratiquer par des méthodes presque artisanales, supposant patience et astuce, comme le démontre la récente découverte par Isight Partner d'une opération (iranienne ?) consistant à piéger 2000 responsables avec de faux sites et de faux comptes[101].

Mais le recours à l'espionnage peut traduire d'autres facteurs que la simple avidité. Ainsi, il faut souvent passer par l'étape de l'espionnage pour développer des actions ultérieures plus

[101] http://www.lemonde.fr/proche-orient/article/2014/05/30/un-faux-site-d-information-utilise-comme-couverture-par-des-espions-iraniens_4428981_3218.html consulté le 29 mai 2014.

offensives. L'opération commence presque obligatoirement par le viol d'un secret - surmonter un pare-feu (*firewall*), obtenir un mot de passe, compromettre un compte, découvrir une vulnérabilité, infiltrer un système, obtenir des informations d'un être humain, surveiller une future cible - et il semble donc qu'il faille « un peu » espionner pour éventuellement frapper « beaucoup ». Par ailleurs, la différence entre espionnage et surveillance mérite d'être analysée.

121 Surveiller (le système de la NSA)

Le système de la NSA représente un exemple inégalable[102]. Officiellement il s'agit d'activités de renseignement, tournées vers le monde extérieur, susceptible de s'intéresser à des citoyens américains mais en respectant le quatrième amendement et s'il y a corrélation entre les messageries de ces citoyens et l'action d'une puissance étrangère. La surveillance serait destinée à lutter contre le terrorisme, la prolifération et les agressions cybernétiques.

Dans la réalité, et s'il faut en croire les documents internes recueillis par Snowden, la NSA pratique, d'une part, des activités de collecte de données et métadonnées sur une base plus ou moins légale et d'autre part des actions totalement clandestines, elles, d'infiltration sur des dispositifs et de vecteurs de messagerie. Par ailleurs, elle pratique à la fois ce que nous avons désigné comme « la pêche au chalut » (intercepter et traiter un maximum d'informations puis trier pour trouver quelque chose de suspect ou de révélateur) et un espionnage ciblé sur des individus précis ou des institutions. Cette double articulation reflète l'ambition du programme, au-delà du prétexte souvent évoqué et guère démontré d'empêcher des attentats.

Le dispositif de surveillance/espionnage est souvent décrit comme « bigbrothérien » (ou « panoptique » par référence au système de prison inventé par Jeremy Bentham et popularisé par Foucault[103]). Or, il ne s'agit pas de s'assurer de l'obéissance de sujets terrifiés à l'idée que rien n'échappe au chef ou au surveillant. En principe secret, le système NSA est moins dissuasif et disciplinaire que prédictif. Il s'inscrit dans la logique d'une *total information awareness* qui préserverait les Etats-Unis de tous les dangers en anticipant les comportements

[102] Il est à peu près impossible de le décrire en détail, tant il est touffu, le plus simple étant de se référer à des animations graphiques en ligne comme « Plongée dans la pieuvre de la NSA » du Monde (le monde.fr), à la « Synthèse du programme de surveillance américain » (linuxfr.org), ou encore au graphique interactif du *Spiegel* (spiegel.de) sur ses outils d'espionnage, tous trois consultés et fonctionnant le 29 mai 2014. Encore faut-il ajouter qu'au rythme où se poursuivent les révélations d'E. Snowden, toute tentative de description risque d'être incomplète.

[103] Notamment dans *Surveiller et punir*, Gallimard, 1975.

des individus et les tendances des masses. Le président Obama a souvent évoqué[104] un nécessaire compromis démocratique entre besoin de sécurité - donc de décèlement - et valeurs de liberté ; mais le système NSA constitue aussi un avantage compétitif dans les rapports géopolitiques ou économiques, au-delà du projet théorique d'arrêter les criminels juste avant le passage à l'acte comme dans le *Minority Report* de Philip K. Dick.

Notre interprétation est que le système répond à la fois à des fonctions classiques de l'interception des messages et de la cartographie des réseaux visant des suspects, à la recherche d'un avantage dans les négociations internationales politiques et économiques (en connaissant d'avance la stratégie du partenaire ou du rival) : donc un très classique espionnage économique. Il nous semble surtout déceler une sorte d'*hubris*, une passion de tout anticiper pour toujours avoir un temps d'avance sur l'événement, en vertu de l'adage que « celui qui sait tout ne craint rien ». Cette quête d'informations stratégiques fait bon ménage avec une autre motivation sécuritaire, conforme à notre hypothèse *hobbesienne* : la peur d'un monde imprévisible. Il y a quelque chose de mystique et de dystopique à la fois dans ce projet de vaincre l'incertitude de l'avenir, notamment en traitant les métadonnées à l'échelon des *Big Data* et en espérant « en savoir plus sur vous que vous-mêmes » via un traitement algorithmique. Celui-ci met tant de facteurs en corrélation que le futur en deviendrait totalement transparent. Si notre interprétation est juste[105], le système américain refléterait un choix fondamental en faveur de la dominance informationnelle et traduirait une mentalité qui sépare les Etats-Unis et le reste du monde comme source de tous les dangers et espace d'une expansion sans fin.

Pour confirmer que les catégories d'agressions ne sont pas étanches, on rappellera les accusations récentes de déstabilisation portées contre la NSA et le GCHQ. Un dispositif voué à la surveillance, mais qui emprunte des méthodes à ses adversaires présumés, les hackers, peut aussi s'étendre à des actions de déstabilisation, technique ou psychologique.

Attaque par déni d'accès (notamment contre Anonymous), création de « pots de miel » pour attirer ses victimes, faux drapeaux (attribuer mensongèrement une agression à quelqu'un), prise de contrôle sur Youtube et Blogger, opérations d'information, dénigrement (propager de l'information négative sur un adversaire de source apparemment neutre), production de faux matériel pour ternir une réputation, désinformation et déception, déni d'accès contre des

[104] Par exemple dans son discours du 17 janvier 2014 présenté sur le site http://whithehouse.gov.
[105] On ne peut pas exclure que la machine NSA ait poursuivi sa propre croissance technico-bureaucratique jusqu'à l'absurde sans réel dessein stratégique.

hackers : à peu près toutes les méthodes offensives semblent être employées, y compris contre des particuliers, activistes ou protestataires.

Que ce soit sur le plan technique (avec les 4 D : *deny, disrupt, degrade, deceipt* : priver, interrompre, dégrader, tromper) ou sur le plan de l'action psychologique, rien ne semble avoir été oublié de la panoplie connue. L'action de l'office des Tailored Access Operations, TAO au sein de la NSA montrerait avec quelle facilité il est possible de passer de l'espionnage « pur » à la déstabilisation.

Bien entendu, les Etats-Unis n'ont aucun monopole en ce domaine : si les agressions présumées chinoises sont essentiellement de l'ordre de l'espionnage, industriel ou politique, rien n'exclut que ces pénétrations ne servent aussi à poser les jalons de futures agressions physiques ou informationnelles.

II Sabotage, ou le besoin de sécurité

2.1 Objectifs

Quels facteurs peuvent pousser à choisir une agression de type sabotage ? Le premier est contextuel : s'agit-il d'accompagner une offensive d'un autre type ?

S'il y a un conflit armé ouvert, il est difficile d'imaginer quelles considérations autres que techniques (crainte que l'offensive ne touche des cibles non désirées ou ne dévoile des panoplies que l'on réserve pour d'autres circonstances) pourraient empêcher de recourir à l'arme informatique pour créer de la confusion dans le camp adverse. Il est au contraire logique d'utiliser tous les moyens d'aveugler l'adversaire et de perturber ses systèmes d'alertes avec des virus électroniques et plus seulement avec des commandos parachutistes. Que la force cinétique appelle de plus en plus comme complément la perturbation informatique ne contredit pas la logique clausewitzienne : augmenter la friction et le brouillard de l'adversaire[106].

[106] Étymologiquement, le sabotage est une méthode qui consiste à travailler « comme un sabot » et, par exemple, à mal entretenir les machines pour punir les patrons des mauvais salaires.

La question se pose différemment lorsqu'il est question de ne frapper l'adversaire que par le seul sabotage informatique. Il s'agit alors d'une méthode de pression (provoquer un dommage chez l'adversaire jusqu'à ce qu'il cède à une revendication politique ou renonce à un comportement), d'avertissement (ce qui à peu près la même chose, mais dans l'optique de décourager les projets adverses plus en amont et de façon plus générale) et enfin de rétorsion (démontrer *a posteriori* à l'agresseur que le prix à payer ne valait pas l'avantage acquis).

Tout cela semble tentant, surtout pour une grande puissance qui pourrait montrer sa résolution sans risquer de pertes humaines ou provoquer de réprobation trop violente de l'opinion publique. Le sabotage cyber pourrait également servir à secourir des forces amies sur le terrain plus sûrement qu'en leur fournissant des missiles dont on ne sait où ils finiront.

2.2 Limites

Pourtant il est des cas où une puissance fait le choix de ne pas recourir au cyberespace.

Pour la Libye, les autorités militaires occidentales paraissent avoir renoncé au sabotage cyber au profit de frappes classiques promises au succès en tout état de cause.

Il est permis de se demander pourquoi les Etats-Unis n'ont pas déclenché de cyberagressions contre la Syrie. Il y aurait eu débat, suivant David Sanger[107] ; les arguments pour l'abstention auraient été :

- la difficulté de choisir les bonnes cibles, donc ne pas frapper la population, ni d'enclencher des opérations qui ne serviraient à rien si elles ne sont pas suivies d'usage de la force sur le terrain. Sans oublier le risque de « bavure » sur des pays neutres ou alliés.
- la crainte de l'effet boîte de Pandore. Cela fournirait un alibi à d'autres puissances. Banaliser ce type de pratiques dans le répertoire des stratégies envisageables en dessous du stade de la guerre, ce serait à la fois donner un argument à des concurrents et stimuler les sentiments antiaméricains en apparaissant comme les grands pirates informatiques de la planète.
- d'éventuelles conséquences juridiques et, dans tous les cas, des accusations qui fuseraient dans les arènes internationales

[107] « Syria War Stirs New U.S. Debate on Cyberattacks », *The New York Times*, 24 février 2014.

Au moment où nous écrivons, ce débat semble se reproduire à propos de l'Ukraine[108], avec ce facteur supplémentaire que la cible potentielle est cette fois russe, donc capable de riposter à une tout autre échelle que la Syrie.

Là encore, il n'est pas facile de savoir ce qui se dit au Pentagone ou à la Maison blanche, et les rares textes sur le sujet rappellent que de telles opérations ne pourraient être révélées - même pas leurs noms de code, ni *a fortiori* leur nature ou de leur effet- serait top secret.

Les stratèges énumèrent les effets attendus de telles agressions : « interrompre, supprimer, dégrader, falsifier, perturber, contrôler ou détruire l'information », toucher des cibles indispensables aux adversaires (réseaux de commandement, de contrôle, aériens, logistiques, opérationnels).

Or, dans ce cas aussi, l'innovation stratégique se heurte au dilemme du choix des cibles ; en l'occurrence, comment produire un effet de chaos qui perturbe le processus de décision adverse mais qui, en même temps, ne touche pas des hôpitaux, des lieux de culte, des approvisionnements énergétiques, des services d'urgence ou autres cibles interdites, et soit « juridiquement » acceptable ? Revoilà la boîte de Pandore : révéler la puissance de ses panoplies et risquer le discrédit qu'entraînerait leur usage n'est-il pas un mauvais choix ?

Ce débat révèle un paradoxe de la puissance. D'un côté le cyber est sensé fournir des armes non létales et un moyen de contrainte, se gérer par écrans interposés, permettre le dosage des effets, correspondre à des sociétés confiantes en la technologie. Bref, elles sont supposées représenter un saut qualitatif décisif et renforcer encore le fort. De l'autre côté, face aux situations concrètes, les stratèges semblent penser que ce ne soit jamais le moment, qu'il n'y ait pas vraiment de cibles adéquates, que les conséquences seraient mal maîtrisées ou qu'il serait toujours trop tôt pour dévoiler ses batteries. Si bien que l'outil merveilleux reste au placard et, pire encore, ce sont les « faibles », les acteurs non étatiques, les présumés « proliférants » ou « voyous » qui finissent par les employer.

La façon de raisonner change si l'on se place du point de vue des Russes. Dans le cas de l'Ukraine, des accusations ont été lancées contre la Russie : occupation de centre de communication en Crimée UKRTelecom JSC, déni d'accès, dégradation de fibres optiques, coupure de réseaux de mobiles, impossibilité provoquée d'accéder aux groupes pro-ukrainiens

[108] Voir « Cybercrimée, la cyberguerre à laquelle vous échapperez peut-être aussi », http://Huyghe.fr/actu_1221.htm, consulté le 27 mai 2014.

sur le réseau social Russian VK. Mais plupart de ces actions restent soit physiques et classiques (faire occuper des centres de communication par des hommes en armes n'est pas très nouveau) soit relèvent de la censure. Et, dans tous les cas, elles sont secondaires. Quand les choses se jouent déjà dans la rue, dans les urnes et sur les écrans de télévision, le cybersabotage n'est pas nécessairement le choix prioritaire.

Plutôt qu'en termes de « scrupules » qu'éprouverait telle ou telle puissance à recourir au cyber, il faut penser en termes de territorialité. Si les Etats-Unis peuvent envisager assez froidement l'envoi d'un virus à l'autre bout du monde, la question se pose différemment pour Moscou. La doctrine russe de « guerre globale de l'information », les enjeux passionnels et idéologiques d'un affrontement qui est aussi une lutte pour l'image plaident pour un recours à tous les moyens disponibles. La révélation de l'affaire *Snake*[109] - des moyens informatiques offensifs dont se seraient doté les Russes de frapper l'Ukraine le jour où cela s'avérerait nécessaire, sur le modèle de la Géorgie, mais qu'ils conserveraient pour le moment - est compatible avec cette hypothèse.

23 Sabotage ou l'avantage du temps

Le sabotage, même au sens le plus strict de dégradation délibérée des capacités techniques et de communication, reste un moyen d'affaiblir l'autre. Encore faut-il savoir à quelle échéance et pour quelle durée. Si l'on part du principe que le dommage sera forcément réparé un jour, le sabotage fait surtout perdre du temps à la cible. Sa duré varie : indéterminé dans le cas de Stuxnet (temps de retard d'un projet de recherche), quelques jours dans le cas de l'Estonie (simple agression par déni d'accès), plusieurs semaines dans le cas de Shamoon.

La bonne question est donc : que fait l'agresseur de ce temps ? S'il s'agit d'un temps de réaction dans le cadre d'une attaque militaire, la réponse est évidente : la durée qui compte est celle de vulnérabilité de l'adversaire. Que les Etats-Unis aient eu intérêt à ralentir la nucléarisation de l'Iran avec Stuxnet plutôt qu'avec des missiles est assez clair. Pour Shamoon, le temps perdu s'est certainement mesuré en millions de dollars. En revanche, nous serions en peine de quantifier les dommages subis par l'Estonie et surtout de les comparer aux avantages politiques qu'elle a retiré de son statut de victime. Le « temps perdu par l'autre »

[109] L'information la plus reprise vient, une fois de plus, de David Sanger et du *New York Times* (9 mars 2014) : http://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html?_r=0

vaut très exactement ce que l'on fait dans l'intervalle : avancer ses chars, exercer une pression diplomatique.

III Subversion, ou la recherche de réputation

En quoi le besoin de reconnaissance pousse-t-il à pratiquer une agression subversive ?

31 Formes et objectifs de la subversion

Plaident en ce sens, toutes les agressions qui sont accompagnées d'une forme de marquage ou de signature, *a fortiori*, celles qui suscitent vantardises publicitaires et autocélébration sur le ton « L'Armée électronique syrienne est passée par là », « *Anonymous* peut vous frapper quand il veut ». Les spécialistes des cyberagressions n'ont pas un ego moins développé que les autres. Les analyses des motivations des hackers citent souvent la volonté de réaliser un exploit ou de gagner du prestige par sa performance. C'est vrai et il faut sans doute élargir la notion au-delà de la satisfaction narcissique qui consisterait à voir son « œuvre » appréciée par ses pairs, voire par les communautés en ligne et les médias.

Internet constitue une arène, un espace où se déroule une compétition entre individus et groupes passant des alliances, provoquant des adversaires privilégiés, affinant des techniques, gagnant de la réputation. Et la question du niveau de la réputation technique des acteurs est tout sauf secondaire[110].

Outre le besoin d'affirmation de soi et de « publicité » pour son équipe, cette lutte pour la notoriété comporte une face négative. Ridiculiser, humilier l'adversaire - qui apparaît alors incapable d'empêcher la présence d'un tag sur son propre site, paralysé par un déni d'accès, hors d'état de conserver ses données confidentielles qui circulent sur la Toile - , bref, attenter à la réputation de la cible, c'est transformer un fait technique - nous leur avons dérobé tel document, nous avons pénétré dans tel système - en message symbolique.

[110] Voir les débats déjà évoqués sur le niveau supposé de la SEA et les tentatives de la ridiculiser par des hackers anti-Bachar. L'histoire d'un supposé piratage de la SEA suivant le principe de l'arroseur arrosé est racontée sur http://reflets.info/opsyria-syrian-electronic-army-was-hacked-and-d0xed-warning-explicit-content/, consulté le 28 mai 2014.

La subversion vise comme l'indique son étymologie à renverser ou retourner un certain ordre, ce qui ne peut se faire qu'en jouant sur des représentations mentales, en gagnant du prestige pour un camp et ses valeurs, en diminuant celui de l'autre. Attaquer est aussi démontrer la fragilité, le manque de légitimité ou les mensonges de la cible. Ceci résulte du contenu du message (l'énoncé) des conditions de l'énonciation : elles traduisent un rapport de force puisque le message est passé en dépit des efforts ou défenses adverses.

Écrire sur son propre blog ou dans son réseau social, c'est exercer une simple liberté d'expression, réprimée dans certains pays. Apposer un slogan pro Poutine sur la page d'accueil d'un hebdomadaire européen social-démocrate ou lui dessiner les moustaches d'Hitler sur *Ria Novostni*, revient à utiliser des outils techniques pour « envahir » une zone numérique. Ici, il est vraiment permis de parler de subversion puisque celle-ci suppose suppose des actes interdits ou qui sapent une autorité.

Nous disions plus haut qu'il est difficile de faire du sabotage numérique sans le précéder par « un peu » d'espionnage ; de même, une action subversive dans le cyberespace doit peu ou prou comporter « un peu » de sabotage. Il a bien fallu franchir un obstacle protecteur, détourner un système d'information de sa finalité, violer des règles, faire un minimum de hacking, ou, pour le moins, emprunter une identité pour parvenir jusqu'à sa cible. Ce qui pose la question : est-ce du sabotage, est-ce de la subversion ?

Plutôt que de ranger un certain type de technique dans une catégorie (par exemple les DDOS relèveraient systématiquement du sabotage et les tags de la subversion), mieux vaut faire un ratio dommage concret/dommage symbolique pour savoir où mettre le curseur.

Pour reprendre des cas déjà évoqués quand Shamoon bloque pendant plusieurs semaines 30.000 ordinateurs d'Aramco, même si l'agression est accompagnée d'un message, il s'agit bien de sabotage. Mais quand, en janvier 2012, pour protester contre la fermeture de Megaupload, les Anonymous s'en prennent au site du FBI et de la justice américaine, puis à la présidence de la République française (pour son soutien à la fermeture de Megaupload et pour Hadopi), et même le site de *l'Express*[111], chacun comprend bien que le but n'est pas de provoquer la paralysie du FBI ni la faillite de l'hebdomadaire, mais de punir symboliquement des responsables d'actes ou propos « liberticides » et de les ridiculiser, typiquement un cas de subversion.

[111] En février 2012, les Anonymous ont bloqué le site de l'Express en riposte à un article de Christian Barbier les critiquant.

32 Les acteurs de la subversion

La subversion paraît logiquement l'arme du faible, du dispersé ou de l'inorganisé contre des cibles hyper-visibles comme des États ou de grandes entreprises, mais cette règle n'est pas absolue. Le fort peut imiter « intelligemment » le faible et mobiliser ses propres hackers pour provoquer désordre ou dérision dans le camp adverse. Le cas de l'Armée électronique syrienne est exemplaire à cet égard, mais en Chine, en Russie ou dans d'autres pays pas nécessairement autoritaires, un État peut décider non seulement d'exposer son propre argumentaire sur Internet et sur ses propres réseaux sociaux (ce qui est de la communication et de la propagande, mais non une agression), mais aussi d'aller défier l'adversaire sur ses propres médias. Outre Tsahal qui pratique cette méthode, les Etats-Unis ont commencé à porter la contradiction sur le terrain de l'autre. Ainsi, le Département d'Etat, déjà convertis à la « *Tweet diplomacy* » sous Hillary Clinton[112], semble *troller,* au sens de se conduire comme le perturbateur qui intervient dans les discussions pour y porter un point de vue violemment critique, ses adversaires. Le compte @ThinkAgain_Dos interpelle ainsi des pro-jihadistes en les traitant d'assassins de femmes et d'enfants. L'idée est de les faire renoncer à passer à l'acte (*think again, turn away*) en leur faisant littéralement honte.

De telles tâches doivent-elles nécessairement être confiées à des êtres humains, comme c'est le cas en Chine où les internautes « patriotes » qui interviennent sur les forums et réseaux sociaux pour soutenir le point de vue de Pékin seraient payés une somme dérisoire « cinq maos », une petite fraction de yuan ? L'idée du logiciel persuasif d'attaque ou du robot « argumentaire » qui décélérait mensonges et désinformation adverses et y riposterait par un discours persuasif est déjà dans l'air depuis quelques années.

On voit ici combien la gamme d'intensité des cyberagressions est étendue. À son apogée, elle correspond à une offensive pouvant faire indirectement de vrais morts ou à des actes de malveillance contre des infrastructures vitales d'une telle intensité que certains y voient un équivalent de la guerre. Dans un registre mineur, c'est l'équivalent numérique d'une peinture sur un mur ou d'une distribution de tracts et à ce stade ne se distingue guère de la simple expression d'une opinion.

[112] On parle aussi de *digital diplomacy* ou *E-diplomacy*, et autres notions présentées par des sites comme http://diplomacy.edu. Il n'est pas indifférent que ce mouvement se soit développé sous Hillary Clinton qui se présente comme une disciple du doyen Nye, créateur des notions de *Soft, smart* et *cyberpower*.

Une agression par sabotage prend son sens soit au service d'une offensive menée par d'autres moyens, soit pour envoyer à un adversaire un avertissement sérieux. D'une opération de subversion, on attend rarement qu'elle renverse un régime à elle seule, ni même qu'elle produise des effets très mesurables, au-delà de son premier impact médiatique. Elle peut être menée sinon par une foule, du moins par des acteurs dispersés voire dissimulés. Enfin elle prend surtout son sens en changeant une « atmosphère », un rapport de domination psychique ou d'autorité, elle modifie l'espoir de victoire entre deux camps. Cela ne se fait pas en une fois, même avec les meilleurs logiciels du monde.

IV Après l'agression : les effets symboliques

Toute agression connue, a un impact psychologique ou sémantique. Car le premier message qu'elle véhicule est qu'elle existe. Ceci implique :

- La preuve d'une vulnérabilité. Dans un monde techniquement parfait, les pare-feu repousseraient toute tentative d'intrusion, les maliciels seraient repérés et désarmés, personne ne perdrait ses privilèges légitimes sur son système de communication etc..
- La démonstration d'une capacité. S'il y a eu agression, quelqu'un était en mesure de réaliser un « exploit » et possède une certaine « force ».

Ces deux informations sont évaluées de façon aussi subjective que le dommage. Cela augmente la difficulté de deviner ce qui pourrait se passer la fois suivante. Ainsi si les défenses bâties entre temps se révéleront efficaces, ou si l'adversaire attaquera une seconde fois autrement ou avec des virus améliorés après un premier essai, etc. Faiblesse des éléments objectifs de jugement et divergence des réactions psychologiques ou stratégiques : autant de facteurs qui renforcent l'impact symbolique de l'agression.

41 Menace et incertitude

La perception de la menace (le dommage possible) et l'incertitude[113] relative à sa vraisemblance ou sa finalité déterminent le comportement des acteurs.

[113] Nous avons développé la notion de croissance paradoxale du secret et de l'incertitude sur Internet dans « Zones d'ombre dans le Cyberespace », numéro d'Octobre 2013 de *l'Observatoire géostratégique de l'information* (http://iris-france.org/analyse/obs-géostratégique-info.php). Voir aussi : http://Huyghe.fr/actu_1201.htm , consultés le 29 mai 2014.

Dans la mesure où la menace suppose l'étalage de la force, il est difficile de le qualifier de stratégie d'influence. Si quelqu'un pointe un fusil, nous ne dirions certainement pas qu'il cherche à nous influencer. Mais dans le monde cyber, il existe plusieurs scénarios.

Le cas plus simple est la menace directe explicite, du type « la bourse ou la vie ». Dans le cybermonde suppose un conditionnel plus subtil « si vous ne faites pas A, vous subirez B », mais, du fait des difficultés d'attribution, ni A (l'enjeu) ni B (le risque) ne peuvent être formulés de manière précise et authentifiée, ils demandent à être devinés.

En cas de chantage pur et simple, l'agresseur demande une rançon à sa cible pour ne pas activer un virus plus dangereux encore que celui dont il a fait la démonstration. Mais ceci relève de la cybercriminalité et non de la cyberstatégie.

Dans les rapports géopolitiques où un gouvernement ne peut faire formuler une menace d'emploi de maliciel par son ambassadeur ni dans la presse.

Quand les agressions sont accompagnées d'un message[114], il ressemble souvent moins à une menace ouvrant la voie à une négociation (comme les communiqués de type « libérez nos camarades ou nous poserons d'autres bombes ») qu'à une punition. L'idée que la cyberagression est le châtiment d'un crime de l'agressé ou la preuve apportée au monde entier la gravité de ses fautes est une constante des communiqués des Anonymous et d'organisations similaires.

42 Puissance, influence et dissuasion

Un autre cas de compromis entre puissance et influence, force pure et action psychologique, se retrouve dans le cas de la dissuasion. L'idée d'appliquer au cybermonde des concepts hérités de la Guerre froide et de trouver des équivalents cyber de la « destruction mutuelle assurée » ou de la « première frappe » remonte au moins aux années 1990 et aux textes précurseurs d'Arquilla et Ronfeldt[115]. La décision d'attaquer - toujours par espionnage, sabotage ou subversion - peut être freiné par la dissuasion mais il peut aussi exister des attaques/démonstrations qui servent à dissuader.

[114] Ce qui est souvent le cas pour des opérations de sabotage ou de déstabilisation par des groupes militants.
[115] Toujours disponibles (en mai 2014) sur leur lieu d'origine, le site de la Rand Corporation.

La dissuasion suppose une posture plus générale que la menace (exigeant quelque chose de quelqu'un en particulier) : l'affirmation qu'une agression d'un certain type susciterait une réponse telle le calcul risque contre gain éventuel devrait décourager l'agresseur virtuel. La dissuasion agit d'abord dans l'esprit de l'ennemi. Autant que le calcul rationnel portant sur la solidité des défenses qu'il rencontrera ou la violence du châtiment qu'il subira, la conviction de la pugnacité de la cible doit freiner l'attaquant.

Une solide défense, l'étalage de capacités d'identification rapide des agressions voire des agresseurs, enfin une bonne résilience des systèmes informationnels leur permettant de se réorganiser très vite par des dispositifs redondants ont certes un effet dissuasif si l'on pense qu'il est inutile de s'en prendre à une forteresse trop bien défendue. Nous ne sommes pourtant pas persuadés que la défense suffise à en juger par le nombre d'agressions qui visent des pays comme les Etats-Unis ou la Chine, sensément bien défendus.

La dissuasion pourrait être explicite, comme s'il existait un code des peines et châtiments, mais ceci supposerait que le coupable soit identifié et qu'aucun tiers de bonne foi ne conteste la validité du système. Dans le cybermonde, s'enchaîner soi-même en s'engageant à réagir d'une certaines façon c'est risquer, toujours à cause du lancinant problème de l'attribution, soit d'être leurré, soit de lancer une riposte qui choquera des alliés ou des neutres, soit de ne pas oser punir un adversaire trop puissant ou trop bien dissimulé, donc de perdre la face.

Partie II - La réalisation de l'action

Une fois déterminées les intentions, la cyberstratégie passe par un mode d'action (chapitres 7 et 8). Il est confronté à des aléas (chapitres 9, 10 et 11) et son résultat dépend aussi de l'efficacité des messages (chapitres 12 et 13).

Chapitre 7 - Choix de l'identité

Le choix de l'adversaire et surtout sa désignation comme ennemi par une instance politique, contribuent à resserrer les liens communautaires et à répondre à la question de notre propre identité. C'est ici qu'intervient l'opacité fondamentale du cyber. La plupart des cyberagressions posent une question d'identité : usurpation pour les opérations par *botnets*, fausse identité dans le hameçonnage, imitation d'un mouvement d'opinion par des algorithmes, sont autant d'exemples de ces difficultés d'identification. Comprendre l'identité dans le cyberespace requiert donc des catégories plus fines que « connu ou inconnu ».

I La question de l'identité dans le cyberespace

11 Identité numérique

L'identité de l'individu, se réfère au caractère unique d'une personne mais peut se décliner en plusieurs composantes comme[116] :

- l'identité légale (ou documentaire) tracée par les passeports et autres cartes d'identité ;
- l'identité contractuelle (cartes de membre, numéros identifiant, cartes bancaires) ;
- l'identité biométrique (empreintes digitale, voix, profil ADN, fond de rétine) ;
- l'identité biographique (mariage, naissance, nom, cicatrices, voire casier judiciaire ou carnet militaire) ;
- l'identité résidentielle (adresse, numéro de téléphone) ;
- et enfin l'identité numérique (adresse IP, adresse électronique, pseudonymes et avatars, comptes de réseaux sociaux).

Toutes tendent à laisser des traces numériques. Autrefois, on pouvait avoir des cartes de membre d'une association (d'un club, d'une entreprise, d'une société) avec un carton imprimé : désormais, ces cartes comportent quasiment toutes une dimension numérique (bande magnétique, carte à puce) qui relie le membre à une base de données informatisée. De même pour les contrats : si les originaux sont encore sur papier, une tendance croissante encourage la signature électronique (par exemple pour les achats sur Internet). L'identité

[116] Voir Guy de Felcourt, *L'usurpation d'identité*, CNRS éditions, 2011, notamment pp. 105-114.

biométrique qui mesure les caractéristiques physiques de la personne tend à se dématérialiser : si l'on prend encore des empreintes digitales ou des photos avec des tampons encreurs, leur saisie et stockage deviennent numériques. *A fortiori* pour certaines empreintes qui ne sont gérées qu'au moyen d'instruments numériques (empreinte rétinienne, ADN, empreinte vocale).

Ce phénomène a été très tôt perçu, sans être du moins nommé. Dès les années 1970, l'informatisation des bases de données est intervenue dans un contexte d'inquiétude concernant les libertés individuelle notamment quand les services de police ont envisagé de connecter leurs fichiers avec ceux de la Sécurité sociale. Cela a conduit à la création de la Commission Nationale Informatique et Liberté (CNIL) en 1978. Trente-cinq ans plus tard, la fusion des identités numérique s'opère de fait à la fois par leur multiplication dans le cyberespace mais aussi à travers les possibilités croissantes d'analyse statistique (*big data*). Ce que la loi a voulu empêcher, la pratique l'a instauré. Certains auteurs utilisent la notion de projection algorithmique[117]. Chaque jour, chacun interagit avec un ensemble de systèmes numériques. Cela passe par le smartphone, la tablette, le PC, le GPS, les objets connectés mais aussi les caméras de surveillance installées en secteur urbain ou les distributeurs de billets.

Pourtant nous pouvons nous abstenir d'utiliser certains services ou recourir à des procédés de camouflage. Le progrès favorise la numérisation de l'identité, mais fournit également les moyens d'y échapper, au moins localement ou brièvement.

12 L'identité collective

Pour l'instant, ces considérations ne concernaient que l'identité individuelle. La stratégie affecte d'abord des acteurs collectifs, la question de leur identité se pose en termes différents. Ainsi, lorsque la NSA écoute le téléphone de mesdames Merkel ou Roussef, l'Allemagne et le Brésil sont-ils visés ? Mandiant, société privée, agit-elle au nom des Etats-Unis ?

[117] Voir Thierry Berthier, « Projection algorithmique et cyberespace », *Revue internationale d'intelligence économique*, 2013/2 (Vol. 5).

L'inattribution, inhérente aux calculs stratégiques, permet d'abord des altérations de l'identité. À la différence des espaces conventionnels où l'on sait qui est l'adversaire, la nouveauté stratégique du cyberespace se manifeste ici.

II L'identité de l'agresseur

21 Effet sémantique recherché et choix de la posture identitaire

Pour l'agresseur, plusieurs attitudes sont possibles suivant les effets recherchés. Révéler son identité en parallèle à l'agression constitue un choix stratégique, mais pas le seul, puisqu'il existe une gamme étendue de « choix identitaires ». En fait, on ne peut conduire de cyberagression sans choisir la posture identitaire adoptée. Toute action offensive tient compte de l'effet sémantique recherché dont fait partie le choix de la posture identitaire ; calcul pareillement effectué par la victime.

Plusieurs postures sont utilisables de la publicité maximale à la discrétion maximale: revendication, faire-savoir, usurpation, dénégation, silence.

22 Revendication

Un agresseur peut revendiquer son action à titre annexe ou principal. Dans le premier cas, la revendication ne vient qu'après les autres objectifs (espionnage ou sabotage). Dans le cas Shamoon, par exemple, l'agresseur veut d'abord ralentir Aramco, la revendication ne venant que compléter l'action.

Dans l'autre cas, les autres résultats obtenus ne servent qu'à pour soutenir la revendication, l'effet principal est sémantique. Ainsi, l'AES ne semble attaquer que pour se faire connaître, elle et sa cause[118]. Son fait d'arme le plus illustre a consisté à pirater le compte Twitter de l'Associated Press et à diffuser une fausse information *(« Two Explosions in the White House and Barack Obama is injured »*). Immédiatement, le Dow Jones a perdu 136 points jusqu'à ce

[118] Berthier Th. et Kempf O., « L'Armée électronique syrienne : entre cyberagression et guerre de l'information », *Revue défense Nationale*, mai 2014.

qu'AP rétablisse la vérité[119]. Pourtant, l'objectif de l'AES était moins d'affecter les cours de bourse que d'obtenir une certaine publicité.

La performance technologique apparente, la nature de la fausse nouvelle s'attaquant aux symboles du pouvoir américain et les conséquences financières touchaient aux trois piliers de la conscience américaine post-11 septembre : terrorisme, technologie et finance. Wikileaks constitue un cas similaire. Si la communication d'informations sensibles par des complices à l'intérieur ressort à la catégorie « espionnage » des cyberagressions, Wikileaks ne pratique pas l'espionnage au sens classique. C'est une plateforme d'accueil pour informations sensibles, en principe authentiques et révélées par des citoyens ayant des motivations morales. L'espionnage préalable ne sert qu'à alimenter des révélations publiques. La revendication, appuyée sur la réputation de Wikileaks, sert le principe de transparence : révéler aux citoyens ce que leur cachent les dirigeants. Ceci renvoie à une idéologie : nos dirigeants, en principe au service du Bien commun, détournent le pouvoir à leur profit ou commettent des fautes qu'ils veulent cacher. Leur activité peut être assimilée à un complot dont il existe des preuves numériques. Les *whistleblowers* nous les fournissent et nous les publions ce qui permet au citoyen au moins de savoir ce qui se fait en son nom. La revendication accroit le prestige de Wikileaks et motive de nouveaux contributeurs.

23 Faire-savoir

Le faire-savoir peut assurer une revendication indirecte de l'agression. Ainsi, lorsque l'existence de Stuxnet est rendue publique en 2010, son niveau technique fait dire aux spécialistes qu'il est l'œuvre d'une grande cyberpuissance. Vu la cible, l'Iran, les soupçons se portent vers Israël et les Etats-Unis.

À l'époque, les deux gouvernements démentent. Deux ans plus tard un article[120] de David Sanger dans le New York Times révèle l'opération Olympic Games et confirme qu'Israël et les Etats-Unis ont été associés à sa fabrication. Or, ces révélations interviennent moins de six mois après que les Américains aient rendu publique leur nouvelle doctrine en matière de cyberopérations qui affirmait le principe d'actions offensives dans le cyberespace.

[119] Voir par exemple http://www.theverge.com/2013/4/23/4257392/ap-twitter-hacked-claims-explosions-white-house-president-injured

[120] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2&pagewanted=all&

Instrumentalisé ou pas par le Pentagone qui dément son implication, D. Sanger a crédibilisé la doctrine stratégique récente. En laissant révéler Olympic Games, sans le revendiquer officiellement, les Américains montraient le sérieux de leur position. A savoir la capacité de se doter d'armes offensives de très haut niveau, de les mettre en œuvre et d'appliquer leur nouvelle doctrine.

24 L'usurpation d'identité

L'usurpation d'identité est un des stratagèmes les plus classiques. Le cyberespace s'y prête par l'opacité et l'inattribution. Rien de plus facile que de détourner les soupçons de la victime et donc d'éventuelles ripostes.

L'affaire de l'agression de l'Elysée en mai 2012 est représentative des problématiques liées à l'usurpation d'identité. Au début quelqu'un prend contact avec des personnes travaillant à l'Elysée et les sollicite comme des amis sur Facebook sous une fausse identité. Puis, ils sont invités à se connecter sur un faux intranet reproduisant celui du palais et où ils fournissent identifiants et mots de passe. Le 11 juillet 2012, Jean Guisnel, spécialiste des questions de défense, la révèle dans Le Télégramme de Brest[121], évoque la piste des « alliés ». Le 20 novembre 2012, l'Express révèle que les Etats-Unis en seraient les auteurs[122], ce que leur ambassade dément « catégoriquement ». L'affaire rebondit lorsque Le Monde rend public un des documents fournis par E. Snowden[123] selon lequel deux hauts responsables français se sont rendu à Fort Meade le 12 avril 2013 pour demander des explications dix mois après l'opération proprement dite. Comme le suggérait l'article de *l'Express*, les autorités françaises soupçonnaient les Etats-Unis, compte-tenu du niveau technique de l'opération. Ces derniers nient mais laissent entendre qu'il s'agit d'un autre pays (éventuellement Israël).

[121] J. Guisnel, « Cyber-agressions. L'appareil d'État visé à deux reprises », 11 juillet 2012, http://www.letelegramme.fr/ig/generales/france-monde/monde/cyber-attaques-l-appareil-d-etat-vise-11-07-2012-1770008.php

[122] « Comment les Américains ont piraté l'Elysée », 20 11 2012, http://lexpansion.lexpress.fr/high-tech/cyberguerre-comment-les-americains-ont-pirate-l-elysee_361225.html

[123] « Comment Paris a soupçonné la NSA d'avoir piraté l'Élysée », 25 octobre 2013, J. Follorou et G. Greenwald.

25 Dénégation et silence

La dénégation est la pratique la plus courante. Elle repose sur une réalité incontestable, il est impossible de prouver qui a conduit une telle opération. Il suffit de nier, une fois les faits connus.

Le silence est la dernière attitude possible. Ainsi, dans le cas de l'affaire Moonlight maze en 1998, les Etats-Unis ont soupçonné les Russes. Malgré les allégations de la presse américaine, la Russie n'a jamais répondu. Le silence semble acceptable lorsque la mise en cause est faible. Quand elle est plus insistante il faut revenir aux autres types de réponse précédemment décrits.

III L'attitude de la victime

La victime dispose elle-même d'une gamme d'attitudes : la publicité, l'acceptation, la manœuvre, la dénégation et le silence.

31 Publicité

La victime assume son statut de « victime » et son identité. Mais il existe plusieurs façons de procéder. Elle peut être plus ou moins discrète. Quand Areva subit une agression en 2011, elle n'est révélée par un article de l'Expansion que quinze jours après la découverte des faits, juste le temps de mettre un terme aux rumeurs. Le discours est apaisant : aucune donnée stratégique n'a été dérobée, l'agression a touché un réseau secondaire. Le délai s'explique ici par le besoin d'examiner les dégâts et de combler les défauts repérés avant de communiquer. Une telle publicité contrôlée est rare et la plupart des entreprises préfèrent garder le silence.

D'autres entités préfèrent jouer d'une certaine publicité. En mars 2009, après une enquête longue de dix mois (juin 2008 à mars 2009), le cas Ghostnet est révélé par une équipe de chercheurs constituée autour de l'Information Warfare Monitor (IWM). D'autres équipes ont ensuite produit des rapports complémentaires (Université de Cambridge). Le 29 mars 2009, le New York Times publie un article sur Ghostnet[124]. La volonté des Tibétains de rendre

[124] *New York Times*, John Markoff, 28 mars 2009, Vast spy system loots computers in 103 countries. http://www.nytimes.com/2009/03/29/technology/29spy.html?hp=&adxnnl=1&adxnnlx=1238324485-jp5DsPj+Ilp5QkMp+k2sMg

publique l'affaire leur permet de se poser en victime et de désigner la Chine comme agresseur[125]. D'où un bénéfice auprès de l'opinion publique occidentale ; la publicité transforme l'agression technique en contre-attaque sémantique.

32 Acceptation

Une autre méthode, face à une agression visible consiste à ne reconnaître que des dégâts mineurs sans s'étendre sur le fond des opérations. C'est souvent conforme à la réalité même si ce semi-aveu peut aussi cacher des atteintes plus sérieuses à la sécurité.

Reconnaître qu'on a été agressé tout en présentant les dommages comme secondaire sert à rétablir une certaine opacité pour renforcer sa sécurité.

33 Manipulation

Un dernier exemple montre l'utilisation de la publicité. En décembre 2010, le ministère français des Finances repère des malversations. En janvier 2011, il porte plainte contre X pour « intrusion dans un système de traitement de données informatiques ». L'affaire est révélée le 7 mars 2011, lorsque le réseau a été sécurisé. Le but est de donner l'exemple mais aussi d'inciter les Français à prendre conscience du risque cyber : si même l'État est attaqué et le reconnaît, chacun doit se méfier.

Si la Chine est initialement désignée comme suspecte, le Journal du dimanche en octobre 2013 suggère que cette accusation aurait servi de leurre pour cacher l'implication de la NSA. La victime peut désigner celui qu'elle croit sincèrement être l'agresseur, mais aussi pointer vers un autre.

[125] Les chercheurs ont identifié quatre serveurs de contrôle et six ordinateurs de commande. Plusieurs adresses IP ont été identifiées sur l'ile de Hainan, en Chine du sud. Trois des ordinateurs de contrôle sont basés en Chine (Hainan, Sichuan et Guangdong), le quatrième aux Etats-Unis. Pour les ordinateurs de commande, l'un est basé à Hong Kong, les autres en Chine (Hainan, Sichuan, Guangdong et Jiangsu). L'ile de Hainan accueille l'état-major du bureau de renseignement de Lingshui et le 3ème département de l'Armée Populaire de Libération (APL). D'autres traces mènent à Chongqing, lieu d'une importante communauté de hackers, non loin d'implantations techniques de l'APL. Toutefois, il n'y a pas de preuve directe de la participation de Pékin dans l'organisation ou l'exploitation de Ghostnet.

34 Dénégation

La dénégation est une des attitudes les plus répandues. Par exemple, dans l'affaire itsoknoproblembro, des institutions bancaires américaines ont été attaquées par DDOS, en 2012, avec une revendication par le groupe Izz ad-din al Qassam Cyberfighters, avec une configuration très rare : celle de l'annonce préalable à l'agression. La plupart des banques américaines ont été ciblées au cours des trois vagues (septembre et décembre 2012, mars 2013), pourtant, très peu le reconnaissent.

35 Silence

Une des pratiques les plus répandues consiste à se taire. La plupart des agressions contre des organisations étatiques ou privés ne sont pas révélées souvent pour entretenir la crédibilité de l'institution. Se dire agressé revient à avouer une fragilité. Le mythe de la sécurité absolue et de la solidité demeure à la base de bien des stratégies de réputation. Un autre calcul est concevable ; en ne déclarant pas les résultats de l'attaque, l'agressé peut espérer remonter la piste. Ces problématiques de révélation sont au cœur des débats actuels sur les déclarations d'incidents. Le dernier Livre blanc recommande de le faire auprès de l'ANSSI qui garantit le secret. Un tel partage contrôlé repose sur la confiance. Chacun étant sensé avoir une certaine confiance dans ses autorités nationales, la question est plus sensible dans le cas d'autorités supranationales. Ainsi, la France est très réticente face aux recommandations du projet de directive européenne de cybersécurité ; ce dernier recommande la déclaration d'incidents au CERT européen ce qui reviendrait à informer des concurrents potentiels ses fragilités.

Chapitre 8 - Choix des cibles

La spécialisation des agressions par secteurs implique la recherche d'un effet maximal suivant le type d'agression (espionnage, sabotage, subversion), mais aussi en fonction des vulnérabilités des organismes ciblés, États entreprises, ou autres. Dans un univers technologique parfait où les pare-feux seraient infranchissables, les mots de passe introuvables, les données totalement sécurisées, la question ne se poserait même pas et il n'y aurait pas de cyberstratégie. Derrière toute agression, il y a une faiblesse d'origine humaine, que ce soit une ligne de code mal conçue par un ingénieur ou une réaction naïve d'un employé.

Le choix de la couche du numérique à viser pour lancer son opération obéit à une logique assez simple. L'agresseur tendra à :

- passer par la couche matérielle s'il peut y avoir accès physiquement : en intervenant sur un câble sous-marin ou introduisant un maliciel dans un intranet par une clef USB, par exemple ;
- par la couche logicielle si son niveau technologique est suffisant ;
- par la couche sémantique, ou pour le dire plus simplement à agir sur un cerveau humain si l'opportunité s'en présente. Ce qui peut se pratiquer conjointement à une action dans le domaine logiciel : par exemple, piéger un correspondant naïf par un message trompeur pour l'amener à télécharger le virus.

Mais encore faut-il déceler les failles. Cela pose la question du « périmètre cyber » des organisations, à rapprocher de « l'environnement économique » des entreprises défini dans les travaux de M. Porter. Il faut appréhender globalement le fonctionnement de la cyber-organisation : facteurs internes, externes ou mixtes. Chaque écosystème cyber offre une facilité plus ou moins grande pour cibler certains éléments, découvrir les fragilités des acteurs ou inventer des stratégies limitées dans l'espace. Il existe deux grandes familles de cibles : directes au sein même de l'organisation en fonction de son mode de gestion ou d'autres caractéristiques ; extérieures ou semi-extérieures liées à son environnement immédiat.

I Ciblage direct

La recherche des vulnérabilités d'une organisation implique de comprendre son système cyber et son mode de fonctionnement. Les agressions menées contre le régime iranien comme Stuxnet, Flame, DuQu, Wiper visaient les systèmes de contrôle des éléments industriels. L'effet final recherché était le blocage du programme d'enrichissement d'uranium. Le

système ciblé était celui du centre de Natanz dont dépendaient des automates Siemens chargés eux-mêmes de piloter les centrifugeuses d'enrichissement de l'uranium pour retarder le processus.

11 Ciblage des SCADA

Le ciblage des systèmes SCADA[126] peut s'avérer particulièrement efficace. La multiplication de tels systèmes qui peuvent se piloter à distance induit des vulnérabilités au niveau du contrôle automatisé[127]. Les systèmes SCADA sont souvent déconnectés d'Internet en raison de leur valeur critique pour l'entreprise. Pour Stuxnet, il a fallu une complicité interne à Natanz ; cela fait de cette opération une combinaison action physique/action cyber et permet de relativiser la toute-puissance supposée du cyberespace. Deux vulnérabilités humaines, la première intentionnelle (celui qui a introduit le ver) et la seconde accidentelle (celui qui l'a fait sortir), sont à l'origine de la réussite et de la diffusion du virus. Les opérations contre les SCADA, a priori bien surveillés, requièrent un niveau de technicité très élevé. Même s'il peut s'en trouver de moins et moins bien protégés comme le système contrôle du tunnel routier du Mont Carmel. L'interconnexion croissante entre systèmes pilotés à distance, souvent avec des caméras comporte des risques. Ceci vaut pour des centres de production industriels énergétiques ou chimiques) ou pour ceux qui assurent une fonction plus anodine, comme système de signalisation de la circulation.

Les piratages du drone Predator américain en Irak en 2009 et du drone Sentinel en Iran en 2011 montrent la nature de certaines vulnérabilités. Ainsi la faille dans le système de contrôle du Predator – non-cryptage des liaisons radio – était connue des ingénieurs américains depuis la fin des années 1990, mais jugée non-piratable, et n'avait pas été réparée. Cette faille a pourtant été exploitée en 2009 par les insurgés irakiens pour récupérer les images prises par un drone. En 2011, le piratage du système GPS d'un drone Sentinel – une autre faille connue depuis 2003 – a permis à des militaires de le détourner et de s'en emparer.

[126] Systèmes de contrôle automatisé et d'acquisition de données servant au pilotage automatisé des éléments industriels.
[127] Une table-ronde sur ce sujet était organisée lors du FIC 2013.

12 Ciblage des autres systèmes de l'organisation

Outre les SCADA, d'autres systèmes entrepreneuriaux subissent des agressions cyber. Les réseaux de communication dont les e-mails semblent plus accessibles aux agresseurs, même si les dommages semblent moindres. Shamoon s'est attaqué aux boites mails pour mettre hors service environ 30 000 comptes utilisateurs. La rusticité du maliciel lui-même, produit d'un *reverse engineering* mais avec des fonctions mal-codées, témoigne (selon la société Kaspersky) de la faiblesse technique des agresseurs ; pourtant le résultat fut tout sauf négligeable. Le ciblage relevait-il d'une volonté (paralyser les communications et donc la décision) ou d'une opportunité (choisir le système de communication par défaut car plus accessible que les autres) ?

Les cyberagressions contre les systèmes de communication ou de gestion des entreprises sont propices pour les manœuvres d'espionnage. Par ces systèmes, transitent une grande partie des éléments d'information utiles que peuvent récupérer des agresseurs pour les exploiter ensuite dans des opérations de subversion. C'est ce que montre l'affaire du Climategate, l'intrusion opérée en 2009 dans les serveurs mail de l'université d'East-Anglia pour voler 161 Mo de données ciblées des scientifiques du Climate Research Unit appartenant au GIEC. D'où l'idée de procéder par une opération d'espionnage puis, après tri et analyse des courriels, de l'extraction et de la diffusion des données susceptibles de décrédibiliser le travail des chercheurs et de monter une campagne de subversion, etc. La faiblesse de la protection des systèmes de communication, fréquente dans les universités et les centres de recherche publics, a favorisé cette opération qui a compromis des négociations climatiques internationales[128] à l'ONU, en suscitant le doute sur les travaux scientifiques qui devaient lui servir de base. L'infection des systèmes de communication se retrouve aussi dans les affaires Climategate, Ghostnet, Aurora, Luckycat, Octobre Rouge, Titan Rain.

Il peut être rentable de profiter de contradictions qui se révèlent notamment entre les aspects techniques et les aspects juridiques. Dans le cas de Bluenext, le vol et la revente massive des crédits carbone ont été rendu possibles par un manque de coordination entre le système technique de la bourse européenne du carbone et le système juridique des registres nationaux.

Le vol en janvier 2011 de crédits sur les registres nationaux autrichien, tchèque et grec a donné lieu à leur revente sur d'autres qui n'étaient pas interconnectés au sein d'un système

[128] Le Climategate a même entrainé en 2010 une enquête officielle du parlement britannique pour savoir si les scientifiques ciblés avaient vraiment falsifié et manipulé des données.

unifié pour des raisons de souveraineté nationale. Du coup, le vol n'a pas suscité d'avertissement global et la faille, ajoutée à d'autres soucis de fonctionnement, aboutit finalement à la fermeture de Bluenext en 2012.

Le cas de l'Estonie comporte aussi un élément technico-juridique : le flou juridique qui règne autour de la notion de conflit dans le cyberespace. Quelle position doit adopter une alliance militaire comme l'OTAN si l'un de ses membres est agressé ? La paralysie décisionnelle entrainée par la résolution de cette question juridiquement complexe a conféré une forme d'impunité aux assaillants, aggravée par l'impossibilité de démontrer une implication directe de la Russie.

II Ciblage indirect

Les vulnérabilités d'un système ne sont pas toujours internes. Les cyber-agresseurs peuvent préférer s'en prendre non à l'organisme-cible, mais à des vulnérabilités liées aux matériels qu'il emploie ou à son écosystème.

21 Ciblage de l'écosystème

211 Ciblage des sous-traitants

La première vulnérabilité externe est liée aux sous-traitants et des fournisseurs dans le cas d'entreprises. Le recours à des partenaires extérieurs qui peuvent être en relation avec les systèmes cyber de l'organisation crée une faille souvent négligée dans l'analyse du risque. Dans le cas de Lockheed-Martin, l'intrusion dans les systèmes de l'entreprise en 2011 s'est faite via une faille dans les tokens SecurID de connexion à distance pour les employés en télétravail. Ce problème dû à un fournisseur a permis le vol des données techniques des programmes les plus avancés de l'entreprise (F-35, V-22, THAAD, Patriot-3, etc.). La vulnérabilité qui s'étend aux fournisseurs et sous-traitants pose la question de l'organisation intégrée dans un cyber-système plus global.

212 Ciblage des standards technologiques

De la même manière se pose la question des technologies répandues comme les logiciels Microsoft (systèmes d'exploitation, navigateur Internet). Même si les organisations disposent souvent d'une autre couche logicielle propriétaire, la base de certaines applications les rend

vulnérables. Le cas des technologies duales dans le monde militaire a été mis en lumière lors de l'affaire du virus Conficker. Les systèmes militaires occidentaux fondés sur les technologies Windows, notamment les serveurs Windows 2003 et 2008, ont été les plus fortement affectés par cette infection. Elle a touché les systèmes de communication de la Marine Nationale, d'où la paralysie des Rafale du Charles de Gaulle pendant plus de deux semaines le temps de nettoyer les systèmes. Le recours croissant à des technologies dites duales est source de vulnérabilités dont l'utilisateur final n'est pas forcément conscient mais qui deviennent des failles internalisées pour l'organisation. Celles qui existent dans Internet Explorer auraient ainsi été utilisées en 2010 dans le cadre de l'opération Aurora contre les systèmes de grandes entreprises américaines (Dow Chemicals, Adobe, Northrop-Grumman, etc.) via leurs navigateurs.

22 Ciblage des informations extérieures

221 Cloud (informatique en nuage)

Se pose également à plus long terme le problème d'infrastructures de stockage « dématérialisées » comme les clouds. Ces derniers peuvent être confiés à des fournisseurs extérieurs, comme Google, d'où de nouveaux risques pour les entreprises qui y ont recours. Des cyberagressions comme Aurora ont prouvé la vulnérabilité de Google. Confier des données de valeur à un tiers, hors du périmètre de sécurité de l'organisation, suppose un risque. Le contrôle réciproque de sécurité, le lien juridique entre les parties et l'importance du lieu de stockage physique des serveurs – ils seront soumis à la loi du pays où ils sont physiquement situés –, voilà autant de nouvelles vulnérabilités à la frontière entre l'intérieur et l'extérieur de l'organisation.

222 Réseaux sociaux

Extérieurs aux organisations mais participant à leur écosystème informationnel, les réseaux sociaux sont vulnérables. Dans le cadre d'opérations de hameçonnage ou de hacking, le vol des identifiants de connexion à ces réseaux peut se traduire en perte de réputation voire en perte économique. En 2013 le hameçonnage initial des mots de passe a permis à l'AES de poster une fausse dépêche d'un attentat à la Maison Blanche. L'utilisation croissante de Twitter dans la communication institutionnelle, des États, ONG ou entreprises et la vitesse de contagion sur ce réseau en font un terrain de guerre informationnelle particulier. Des organisations terroristes, Shebabs, Talibans, ou activistes, Anonymous, AES, ou autres

peuvent faire instantanément connaître leurs positions ou diffuser des documents avant la moindre tentative de censure ou de riposte. Twitter peut exploiter des vulnérabilités d'organisations étatiques ou entrepreneuriales. La plateforme peut être utilisée pour une stratégie directe (infoguerre) ou indirecte (vol d'identités / d'identifiants de comptes réels à des fins de désinformation). Le fait qu'il soit très facile d'y utiliser de fausses identités, de faux relais ou organisations ou de faux comptes est un atout de plus pour les attaquants.

Des entreprises ne dépendent pas seulement de leur périmètre économique mais aussi d'un périmètre informationnel qui, à travers notamment la réputation et la circulation instantanée d'informations non filtrées par les médias traditionnels, devient un élément de promotion comme de vulnérabilité. La guerre informationnelle qui inclut les actions de subversion joue un rôle croissant dans le cyberespace. Des médias 2.0 comme Twitter, Youtube ou Facebook, chacun avec sa particularité, rendent les organisations économiques et politiques plus vulnérables à la diffusion de messages destinés à ridiculiser ou dénoncer l'adversaire, y compris quand ils proviennent d'organisations clandestines ou très peu structurées. La guerre informationnelle devient plus particulièrement rentable pour elles et, en miroir, elle rend les organisations établies (États, entreprises) particulièrement exposées.

Conclusion sur le choix des cibles

La découverte et l'exploitation des vulnérabilités des systèmes cyber sont un préalable à l'action, comme dans toute stratégie. Le cyberespace offre des possibilités d'actions qui s'adaptent non seulement au niveau technique de l'agresseur mais aussi au type d'agression souhaité. À la division entre sabotage, espionnage et subversion répond donc une pluralité de cibles (systèmes de pilotage industriel, systèmes d'information).

Une classification des menaces comme celle du DoD prend en compte, outre le niveau d'organisation des agresseurs, le degré de complexité et de notoriété des failles utilisées. Les premiers niveaux correspondent à l'utilisation des failles connues : une attaque peut être reproduite par ceux qui n'auraient peut-être pas été capables d'inventer la première, mais savent copier. Cette remarquable souplesse des méthodes de lutte fait de la cyberstratégie un domaine ouvert par excellence.

Chapitre 9 - Temporalité de l'action

Dans les éléments fondamentaux de toute analyse stratégique, la temporalité des événements occupe une place centrale. La durée de l'action, qui comprend aussi la durée de la planification ainsi que celle de la permanence ou non des effets dans le temps, révèle souvent des éléments essentiels de pensée stratégique de l'agresseur en même temps qu'elle permet une perception du succès ou de l'échec. Son analyse se révèle primordiale pour comprendre également le degré de complexité d'une cyberaction, une longue planification se révélant le plus souvent être l'apanage d'organisations puissantes. La multiplication des agressions ces dernières années permet d'analyser plus spécifiquement la temporalité des différentes actions par la multiplication des cas documentés. En effet la mesure quantitative n'est possible que grâce à l'accélération des cyber-agressions depuis la deuxième partie des années 2000 qui ont mis en avant l'explosion de la conflictualité dans le cyberespace.

I Durée selon les actions

Les analyses menées font ressortir une importante dichotomie entre des actions de temps court inférieures à 6 mois et des actions de temps long pouvant s'inscrire sur plusieurs années. Plusieurs facteurs peuvent expliquer cette différenciation, à commencer par le type d'action envisagé. En effet les différentes cyberactions entraînent des complexités particulières à la temporalité différente. Les trois grands types de cyberagressions qui ont été identifiés par cette étude, à savoir sabotage, espionnage et subversion, obéissent à des temporalités différentes.

11 Le temps du sabotage

Les actions de sabotage semblent être les plus immédiates. En effet une action de cyber-sabotage visant un système de gestion comme dans le cas des boites mails d'Aramco pour Shamoon ou un système industriel de type SCADA comme celui du contrôle de trafic routier du tunnel du Mont Carmel en Israël[129], si elle peut avoir été planifiée en amont, est avant tout un événement à effet immédiat. Entre l'envoi du maliciel et ses effets, il ne s'écoule que

[129] http://www.infosecurity-magazine.com/view/35289/cyberterrorism-shut-down-israels-carmel-tunnel/ ; consulté le 28 mai 2014.

quelques instants et le but même d'une telle agression est d'obtenir des effets quantifiables et visibles, éventuellement exploités par la suite. Ces actions sont ainsi de courte ou de très courte durée, le temps que le maliciel soit intercepté ou remplisse sa mission, avec fréquemment un auto-effacement de ce dernier après action.

12 Le temps de l'espionnage

Au contraire les actions d'espionnage apparaissent comme les plus longues dans le temps. Le but primordial de l'espionnage étant la collecte de données de manière dissimulée, les maliciels utilisés doivent être les plus discrets possibles. Les opérations d'espionnage utilisant principalement des moyens cyber ont pour vocation de contourner les mesures de protection et de se fondre dans le système ciblé. Il en résulte une complexité accrue à remonter jusqu'à l'origine des agressions, y compris temporelle. Plusieurs cas d'étude montrent des manœuvres d'espionnage de longue durée à des fins politiques (Ghostnet contre les réseaux d'activistes tibétains, Luckycat) ou économiques (vol de données du F-35 chez Lockheed-Martin, Octobre rouge) dont il est difficile voire impossible d'estimer la durée exacte ; tout au plus peut-on supposer qu'elles ont duré plusieurs années avant d'être, le plus souvent fortuitement, découvertes. Ces actions révèlent des volontés d'espionnage, le plus souvent par des structures pérennes ou fortement organisées, pour maintenir un système de recueil de données pendant des durées supérieures à 6 mois voire plusieurs années.

13 Le temps de la subversion

Les actions de subversion, quant à elles, s'apparentent à des hybrides entre le temps long et le temps court. Elles regroupent en effet toute une palette de sous-catégories allant de la simple revendication, de temps immédiat après action, aux manœuvres de guerre informationnelle qui sont de temps long et qui consistent à dénoncer les crimes ou les faiblesses supposées de l'adversaire suffisamment longtemps pour le mettre sous pression. Ainsi la « guerre des tweets » en Afghanistan se poursuit-elle depuis plusieurs années dans le but de discréditer la FIAS tant que celle-ci est présente sur le territoire afghan. De même l'action contre GDF SUEZ au Brésil est-elle destinée à durer plus de six mois, le temps que l'entreprise soit suffisamment empêtrée dans cette affaire et qu'elle se retire d'elle-même d'un appel d'offre. Au contraire l'affaire du Climategate est-elle quasi-immédiate entre la mise à disposition sur

des sites climato-sceptiques des données volées au GIEC et leur publicité visant à attirer le plus grand nombre sur ces sites.

Contrairement aux actions d'espionnage qui doivent par essence rester cachées, la plupart des actions de subversion ont pour but d'être le plus rapidement et le plus intensément connues du grand public ou du moins du public-cible. Si l'auteur peut et veut parfois rester anonyme, la logique de publicité de l'affaire en fait régulièrement des actions visibles dont la temporalité est traçable. D'ailleurs l'échec de telles actions vient souvent d'une erreur de positionnement ou de séquençage par rapport à la cible comme OpGabon. Dans le cas d'actions croisées, cela pose également la question de la composante informationnelle de l'action, le plus souvent selon un mode revendication / contre-revendication / dénonciation.

II Temps et stratégie

Il existe un double temps des cyber-actions : un temps propre au cyberespace qui tend au raccourcissement des boucles de diffusion comme le montrent par exemple les opérations menées sur Twitter et un temps plus long, celui de la planification des opérations complexes.

21 Planification

Stuxnet illustre la porosité et la complémentarité entre les différents types d'agressions comme la nécessité d'une planification amont. En effet l'opération Olympic Games à l'origine de la campagne Stuxnet date vraisemblablement de 2006 et a dû être confirmée par la nouvelle administration avant que l'action offensive proprement dite ne soit entreprise en 2009. De même Dark Seoul qui a touché la Corée du Sud en mars 2013 aurait été planifiée plus d'un an à l'avance.

La révélation et l'analyse d'une phase de planification plus ou moins longue permet d'approcher la complexité de certaines opérations, au-delà du fait qu'elles puissent combiner ou non plusieurs modes d'agression. La planification renseigne d'une certaine manière sur le degré d'organisation du ou des auteurs et sur leurs capacités d'anticipation des évolutions cyber de l'adversaire. On retrouve majoritairement cette phase de planification dans le cas d'agressions menées par des organisations étatiques (Stuxnet, Dark Seoul, Opération verger). De plus la combinaison entre différents modes d'agression, par exemple une première phase d'espionnage permettant de comprendre les vulnérabilités de l'adversaire, suivie d'un

sabotage dont le résultat sera exploité par une action de subversion, organise une temporalité particulière et une articulation entre actions complexes qui est la marque des organisations les plus solides.

Dans le cas des agressions de subversion, la planification relève aussi d'une question d'opportunité temporelle. Dans les cas de GDF SUEZ au Brésil et du Climategate, les actions ont été menées en retroplanning par rapport à des dates précises. Dans le cas de GDF SUEZ il s'agissait de l'attribution du contrat du barrage de Belo Monte, prévue à cette époque en octobre 2010 et dans celui du Climategate de la Conférence climatique de Copenhague de décembre 2009. Il s'agissait ainsi de faire peser une pression médiatique énorme sur les cibles pour les discréditer en vue de ces deux dates importantes. L'action de subversion a donc été planifiée dans le temps pour que, selon la cible, la pression devienne maximale au moment choisi. Dans le cas de GDF-SUEZ il s'agissait du forum de Davos 2010 et dans celui du GIEC des semaines précédant l'ouverture de la conférence. Dans le premier cas l'entreprise française a choisi d'elle-même de se retirer du projet et dans le second, les positions du GIEC, base de travail scientifique de la conférence, ont été contestées ce qui a empêché la conclusion de l'accord.

22 La poursuite de l'action dans le temps

La temporalité doit aussi s'envisager dans la continuité de certaines actions qui peuvent parfois s'amplifier. La continuation de l'action, soit par la répétition de plusieurs opérations identiques, ou quasi-identiques, comme la guerre des tweets en Afghanistan ou l'emploi contre l'Iran de Flame, DuQu et Wiper, soit par l'articulation de plusieurs opérations comme lors de la guerre Israël-Hezbollah en 2006 ou Stuxnet en 2009, traduit une gestion de la temporalité particulière. Les actions de très longue durée, se répétant ou s'amplifiant, semblent caractériser de entité étatiques ou du moins des organisations fortement structurées. La question des moyens humains et matériels dédiés aux cyber-actions interfère avec l'analyse de la temporalité.

Le cas Conficker est intéressant puisqu'il met en avant non pas un sabotage destructif réel mais un sabotage putatif. En effet le virus, mis en forme à partir d'une faille Windows, ne cause pas de destruction par lui-même mais crée un blocage des systèmes de protection (antivirus et mises à jour Windows). La durée de plus de six mois pour une action de sabotage

– apparemment sans autre cible finale que les utilisateurs de solutions de systèmes d'exploitation Windows ou Windows Server, natives ou duales – est inhabituelle. Elle est principalement due au fait que Conficker n'est pas un virus isolé mais une famille de virus (désignés Conficker A à E) ayant fait l'objet de mises à jour et de nouvelles versions. Il s'agit ainsi d'une action poursuivie dans le temps, de manière relativement longue pour une action de sabotage, avec la volonté d'adapter l'outil aux éventuelles contre-mesures mises en place puisqu'à partir de la version C, Conficker dispose lui-même d'un module de mise à jour automatique.

III Autres considérations temporelles

31 Durée et efficacité

La question de l'efficacité d'une action semble également liée à sa temporalité, celle de la cible (existence éventuelle d'une échéance particulière) mais aussi celle des actions. Savoir si les actions de long terme sont les plus efficaces implique de déterminer si les organisations les plus puissantes et les plus structurées, seules à même de mener ces actions longues, sont celles qui obtiennent les meilleurs résultats dans le cyberespace ?

L'existence d'actions très ponctuelles (piratage du compter Twitter de l'Associated Press) montre que ces dernières peuvent parfois être extrêmement efficaces. Moins de 20 minutes ont été nécessaires pour faire perdre 143 points à l'indice phare de l'économie américaine. Cette action, revendiquée dans la foulée par l'AES (compte piraté à 13h07, tweet envoyé à 13h10, revendication sur le compte Twitter de l'AES à 13h17) montre l'efficacité de ce type d'actions, pour peu qu'elles soient adaptées à la cible.

Le but de toute cyberaction étant de produire des effets quantifiables dans la vie réelle des cibles, la question du rapport entre durée et efficacité ne semble au final pas si pertinente. La prise en compte majeure doit donc être celle de la dichotomie existante entre le temps du cyberespace et le temps du monde réel, les deux ayant de plus en plus tendance à se confondre. Dans le domaine économique c'est fondamental, avec la dématérialisation de l'économie associée à la transformation des systèmes économiques occidentaux vers une base de plus en large de services et l'apparition de phénomènes de *bots traders* dans le cas du *High Frequency Trading*.

À l'inverse, dans le domaine militaire, c'est en grande partie parce qu'il a été capable de maintenir une action de subversion contre Israël tout au long de la campagne de juillet 2006 que le Hezbollah peut être considéré comme le vainqueur médiatique de la guerre. Chaque action militaire menée par Tsahal était méthodiquement contrée et chaque contre-agression ou victoire – la moindre perte de blindé ou capture de soldat adverse – du Hezbollah était magnifiée via un réseau de relais (blogs et Twitter). Dans ce cas c'est bien la longue durée de l'action cyber, au regard de l'action militaire elle-même, qui a déterminé le succès sémantique du Hezbollah.

32 Décalage entre action et revendication : le temps de l'agitprop

L'élément fondamental de l'action reste son exploitation. La sortie de l'action du cyberespace pour obtenir un effet dans la vie réelle que ce soit la destruction de matériels, le vol de données ou le discrédit d'une personne ou d'une organisation, doit ainsi être le but final de toute cyberagression. Revendication, contre-revendication ou dénonciation occupent une place particulière avec un tempo particulier : ces éléments survenant après l'action proprement dite sont cruciaux dans la cyber-conflictualité.

L'ensemble de ces manœuvres qui s'apparentent ainsi à de l'agitprop quant aux finalités, sont amplifiées par les caractéristiques du cyberespace (vitesse de diffusion, interconnexion mondiale, anonymat relatif). Ainsi, la revendication voire la contre-revendication, offre une forme d'initiative stratégique à l'agresseur. Le résultat est ainsi de montrer la faiblesse de l'ennemi et de le ridiculiser, tactique employée le plus souvent face à des États ou de grandes entreprises dans une posture du faible au fort. Habituellement les revendications sont des actions rapides, pour certaines quasi-immédiates, Epée Tranchante de la Justice revendique Shamoon le jour même de sa découverte, l'AES revendique le piratage dix minutes après sa réalisation.

La dénonciation de l'agresseur est devenue récurrente dans la rhétorique du cyberconflit. En l'absence de revendication claire, la dénonciation devient un élément de contrôle informationnel des conséquences. Il est parfois plus intéressant pour les agressés de révéler une agression et de dénoncer les agresseurs supposés pour conserver l'initiative stratégique. La dénonciation rapide offre ainsi plusieurs possibilités de riposte ou de valorisation géopolitique. Ainsi Google a profité de l'affaire Aurora pour apparaître comme un élément à

part entière de la géopolitique des Etats-Unis. Cela a aussi permis aux Etats-Unis de justifier leur attitude stratégique envers la Chine comme adversaire désigné en ce début XXI^{e} siècle[130]. Les dénonciations prennent place dans une temporalité plus longue que les revendications. Il aura fallu près de deux semaines après l'affaire Aurora pour que les Etats-Unis désignent la Chine et deux mois entre la découverte de Shamoon et la mise en cause de l'Iran par les Etats-Unis.

[130] Un exemple tout récent : l'inculpation d'officiers chinois par la justice américaine au titre de leur cybercrimes supposés et la réaction de Pékin face à « l'hypocrise » de cette démarche : http://www.lemonde.fr/international/article/2014/05/20/cyberespionnage-pekin-accuse-les-etats-unis-d-hypocrisie_4421719_3210.html ; consulté le 28 mai 2014.

Chapitre 10 - Succès ou échec

Que signifie être victorieux dans le cyberespace ? La réussite de la « manœuvre » dans les deux premières couches ? Ou leur exploitation sémantique ? Suffit-il d'une victoire symbolique ? Outre la part de la croyance inhérente à toute victoire, la réponse met en jeu le problème du rapport entre les effets recherchés et le résultat obtenu.

I Conception classique de la victoire

11 Héritage occidental

Selon la doctrine stratégique classique, la guerre est une dialectique des volontés (Beaufre) où chacun fait la loi de l'autre (Clausewitz). Dans les guerres de l'ère industrielle, la victoire ou la défaite sont nettement définies. La première consiste à dominer totalement l'adversaire : guerre de Sécession américaine, guerre franco-prussienne de 1870, guerres mondiales. De même, les guerres de décolonisation sont vitales, du moins pour la partie qui lutte pour son indépendance et qui l'obtient finalement. La victoire fait disparaitre l'ennemi, soit par disparition du chef, soit au renoncement des forces politiques après reddition militaire. Les victoires d'anéantissement ou d'effacement politique ne sont plus la règle des conflits contemporains.

La victoire définitive paraît désormais longue et coûteuse quand bien même de premiers succès militaires sont vite acquis (chute du président, occupation de sa capitale, reddition des armées). La victoire sur le tyran irakien ou libyen ouvre sur une seconde guerre asymétrique de partisans. Il est ainsi possible de parler de la fin du modèle occidental de la guerre[131]. Telle est du moins la thèse de Béatrice Heuser[132] pour qui ce modèle de la victoire absolue est obsolète. D'une façon plus générale, les guerres asymétriques mettent à mal le schéma de la bataille décisive.

[131] Victor Hanson, *Le modèle occidental de la guerre. : la bataille d'infanterie dans la Grèce classique*, Belles lettres, 1990, édition consultée : Tallandier Texto, 2007.
[132] Voir Béatrice Heuser, *Penser la stratégie de l'Antiquité à nos jours*, Editions Picard, 2013.

12 Victoire, succès et complexité

Cette évolution générale n'est pas liée au seul fait nucléaire, mais aussi à une complexité croissante des conflits. Le combat terrestre est devenu plus large (fronts démesurés, apparition de l'échelon opératif, développement du soutien) tout comme le combat naval qui se déroule désormais sur, sous et au-dessus du niveau de la mer ; désormais, on ne conçoit plus de bataille purement navale. Autrefois, ces milieux étaient clairement séparés, aujourd'hui ils se sont rejoints et sont désormais intégrés dans une bulle aéroterrestre ou aéromaritime. S'ajoutent de nouveaux milieux ou sphères stratégiques, rendus possibles par le progrès technologique qui renforce cette intrication généralisée. Les stratèges n'envisagent plus de victoire dans un seul milieu car il y aura toujours moyen de déborder vers un autre pour continuer la lutte. La manœuvre indirecte tend à devenir la règle avec l'interarmisation des combats.

Le succès se détache de plus en plus d'un constat objectif. Le brouillard et la friction altèrent la perception des résultats du combat. Désormais, le succès réside plus dans la conviction partagée qu'il est avéré plutôt qu'en sa réalité objective : la croyance devient aussi importante que sa réalité. Ceci vaut pour les adversaires comme pour le public.

Dès lors, la victoire n'existe que si le vaincu accepte sa défaite. Il faut que les deux parties acceptent le jugement des armes, source d'un nouveau droit qui deviendra leur loi. La victoire possède une double dimension sémantique : ce que se disent les adversaires (reconnaissant ou pas leur défaite, acceptant un compromis) et la façon dont ils le manifestent au public. C'est pourquoi, avant de proposer une théorie du cybersuccès, il convient d'étudier dans quelques cas la relation entre le résultat sur le terrain et le discours accompagnateur.

II Exemples sur l'ambiguïté de la victoire

21 L'opération Verger

L'opération Verger est significative parce que lisible. Un raid de l'aviation israélienne, le 6 septembre 2007, détruit une usine syrienne de recherche nucléaire, probablement à vocation militaire. Les renseignements préalables ont été obtenus par un programme espion. Le raid a été permis par l'aveuglement de la défense aérienne syrienne, grâce à plusieurs moyens

cybernétiques et électromagnétiques. Le résultat est visible : le réacteur est détruit. La manœuvre d'aveuglement a été un succès grâce à des moyens cyber.

22 Hezbollah, fabrication de la victoire

Le Hezbollah a mené plusieurs guerres contre l'armée israélienne, notamment en 2006. Or, si les spécialistes s'accordent à reconnaître qu'Israël a subi relativement peu de pertes et progressé très vite en territoire ennemi, la résilience du Hezbollah qui a continué de tirer des roquettes tout au long du conflit a surpris les observateurs. Ce qui pourrait donc apparaître comme une victoire militaire israélienne est souvent perçu comme une victoire politique du Hezbollah qui l'a célébrée comme telle.

L'utilisation de la couche sémantique par théatralisation d'une victoire plutôt symbolique a une fonction de subversion amplifiée notamment sur les réseaux sociaux. « *Après avoir détruit les roquettes à longue distance de la branche armée du mouvement et les infrastructures civiles du parti de Dieu, le gouvernement d'Ehud Olmert lança une intervention terrestre. Il accentua les frappes contre les infrastructures du pays sans pour autant parvenir à faire cesser les tirs de roquette à courte portée* ». Ainsi, « *du côté libanais, le Hezbollah perdit plus de 600 combattants et ses stocks de roquettes à longue et moyenne portée furent localisés et bombardés presque totalement dès le deuxième jour du conflit* ». Du côté israélien, « *les pertes humaines furent importantes -120 soldats tués- mais l'élément stratégique au cœur de sa sécurité, sa capacité de dissuasion, a été préservé et restauré. (...) Le Conseil de sécurité a reconnu la responsabilité du Hezbollah dans le déclenchement du conflit* »[133].

Le récit construit par le Hezbollah fut propagé et crédibilisé par ses médias dont la chaîne Al-Manar et grâce à son contrôle de l'information. Les combattants du Hezbollah n'apparaissent en effet à l'image qu'à deux reprises. Le reste des images diffusées par les médias classiques ou les réseaux sociaux ne montrent que destructions, civils éplorés et pertes israéliennes. La maîtrise de la source médiatique et l'exploitation de la viralité du cyberespace accentuent cet

[133] Sur lambiguïté de la victoire voir B. Dax, « Le flou de la victoire du Hezbollah en 2006 », *Revue Défense Nationale*, janvier 2014 et G. Blum, « Fog of victory », *European Journal of International Law*, 2013/24, pp. 399-421.

effet. Il transforme une défaite tactique en une victoire symbolique au Liban comme en Israël ou dans la communauté internationale.

23 Stuxnet, succès ou échec ?

Le ver a ralenti le programme nucléaire iranien : succès. Mais il s'est échappé et a été rendu public : échec. Toutefois, la qualité technique du virus a été analysée par certains comme la preuve de la force des auteurs : succès. Pourtant, la découverte de Stuxnet le rend difficile à réutiliser, d'autant que les Iraniens s'investissent dans la cyberdéfense : échec. Deux ans plus tard, une fuite révèle les longues préparations du programme Olympic Games, au moment où les Américains insistent sur leur stratégie de cyberdissuasion : succès. Mais cela fournit un argument pour désigner les Etats-Unis comme le premier cyberpirate du monde : échec. Et ainsi de suite.

Le cas Stuxnet démontre aussi que les manœuvres sémantiques peuvent s'intégrer à l'opération même. Autrement dit, la subversion n'est pas que de la propagande qui toucherait les masses, elle peut aussi être ciblée. C'est ce que suggère Ralph Langner[134]qui, au terme d'une analyse criminologique de trois ans, affirme que Stuxnet serait en fait composé de deux opérations successives. La première variante aurait été introduite en 2007 et servait à ralentir le travail des centrifugeuses et non à les détruire. En provoquant une situation catastrophique, l'agresseur aurait incité l'équipe iranienne à examiner tout le dispositif et à découvrir la déficience logicielle. Donc, le virus devait éviter tout dommage trop spectaculaire, mais provoquer suffisamment d'incidents pour qu'ils aient l'air « naturels », si bien que l'équipe de scientifiques iraniens perdrait du temps à vérifier et essayer des solutions aléatoires[135].

Deux ans plus tard, en 2009, une nouvelle version aurait été implantée, à la fois plus facile à identifier et plus sophistiquée comme si l'auteur avait aussi voulu que ses exploits soient connus. Cela aurait permis aux Américains de prouver leur excellence et de crédibiliser leur nouvelle doctrine cyber, ce que R. Langner nomme un « effet Spoutnik » : avoir été le premier à agir offensivement dans le cyberespace. Si cette double explication est la bonne, elle confirme que quelque soit le niveau technologique de l'action dans la couche logique, l'action dans la couche sémantique est déterminante.

[134] R. Langner, Stuxnet's secret twins, *Foreign policy*, 19 novembre 2013.
[135] Rappelons qu'ils développaient leur programme de façon isolée et ne pouvaient donc faire appel à la communauté scientifique pour comparer leurs résultats.

24 La stratégie du silence

Paradoxalement, l'opacité du cyberespace altère l'exploitation des succès. En effet, dans un conflit classique, sauf opération clandestine, celui qui remporte un succès le proclame. Ce n'est pas forcément avéré dans le cyberespace.

Certaines opérations recherchent la publicité : c'est le cas attaques DDOS ou par publication de documents cachés. Pourtant, la plupart des opérations cyber ont vocation à demeurer celées. En cas d'espionnage, révéler ce qu'on a fait revient à prévenir la victime. La publicité tarit la source d'information. L'espion doit logiquement se taire. Dans une manœuvre de sabotage, l'agresseur accepte le risque que son action soit repérée. Mais il peut aussi calculer un sabotage suffisamment discret pour ralentir les activités de la victime sans que celle-ci ne s'en rende compte. Un sabotage vise alors à entraver durablement quand une action d'éclat n'aura que des effets brefs. En cas de subversion, l'agresseur peut avoir intérêt à ne pas se dévoiler pour ne pas entraver la manœuvre en cours.

25 Opération Gabon : l'échec

En 2013, Anonymous décide d'attirer l'attention sur les crimes rituels commis au Gabon en lançant l'opération OpGabon. Pour cela, le collectif lance le piratage des sites pro-Bongo et quelques défacements de site (Courtage Gabon Logistique, PetroGabon, Comilog, Axa Gabon). L'opération est annoncée le 13 avril 2013, avec l'ouverture d'un compte Twitter @OpGabon .

Force est de constater l'échec de l'opération. Les pétitions en ligne lancées en même temps n'ont recueilli que 2450 signatures. Les mesures d'activité du compte Twitter OpGabon et du #OpGabon sont assez faibles. Peu de grands médias en ligne francophones ou anglophones (1 entrefilet sur France 24) reprennent l'opération. La première partie de l'opération OpGabon devait rester centrée sur le Gabon lui-même, mais devant le relatif échec, le collectif Anonymous a décidé de s'en prendre aux filiales étrangères (surtout françaises) présentes au Gabon pour essayer de faire plus de buzz ; sans beaucoup de succès.

Quelles sont les raisons de cet échec ? Tout d'abord une action marginale sur un pays qui n'est pas au centre des intérêts mondiaux, avec peu de relais médiatiques. Ensuite, une opération qui dure dans le temps mais donne l'impression de ne pas être entretenue.

III Théorie du cybersuccès

31 Des calculs à un coup

La notion même de bataille dans le cyber pose des questions. Dans un conflit classique, les deux belligérants jettent leurs forces dans un affrontement simultané où les actions réciproques se contrarient dans le même temps. Le cyberespace est tel que les actions et les réactions s'enchainent selon un ordre séquentiel. S'il y a contre-agression, elle est décalée dans le temps. L'observateur a du mal à apprécier les résultats puisqu'il faudrait considérer l'ensemble des mouvements d'agression et de riposte pour juger du succès des acteurs.

Malgré l'« universalisation » du cyber, la létalité et la portée concrète des cyberactions restent limitées. En effet, il est difficile d'évaluer l'ampleur d'une opération de cyberespionnage, même si des analyses chiffrent en milliards de dollars le coût global des vols de données pour l'économie. Il n'y a pas encore d'exemple de cybersabotage aux effets décisifs. Quant à la subversion, par définition, ses effets ne sont ni isolés, ni mesurables. On ne peut dès lors envisager que des succès, limités par construction.

32 Vaincre dans le cyberspace ?

Dans le cyber le succès est triplement relatif :

- Opère-t-il dans la seule sphère cyber ou interagit-il avec les autres ? L'agresseur doit très clairement répondre à cette question au moment de concevoir son opération.
- Quel est le « temps espéré » du succès ? Quel horizon temporel se fixe l'agresseur pour mesurer le succès de son opération ? Doit-il prendre en compte les conséquences lointaines ?
- Dès lors, on comprend que dans la plupart des opérations le succès repose sur son exploitation sémantique.

Ainsi, le premier choix consiste à définir si l'opération doit rester dissimulée en fonction de l'objectif considéré. Il faut prévoir une manœuvre sémantique en cas de découverte du secret : que dire si l'opération est révélée ? Si l'on recherche un effet sémantique, qu'il soit principal ou subordonné détermine les modes opératoires. Il s'agit ensuite de qualifier la cible :

restreinte, même en cas d'effet sémantique public (cas du Climategate) ou large (cas de l'Estonie).

Il s'agit de toucher les relais d'opinion comme dans toute guerre de l'information.. Pour le défenseur, l'alternative revient souvent à décider de rendre publique l'agression ou pas.

À la question de savoir si l'opération est un succès ou un échec, il ne semble pas qu'il y ait de réponse assurée. La méthodologie préalable, consiste à intégrer les effets sémantiques recherchés, au moins de façon à ne pas être surpris par les éclaboussures médiatiques.

Chapitre 11 - L'inévitable imprévisibilité

L'imprévisibilité dans le cyberespace renvoie à la notion clausewitzienne de friction. Pour le stratège prussien, la friction regroupe tous les éléments imprévus qui font que le résultat diffère de sa conception théorique. Trois aléas majeurs peuvent être à l'origine de l'imprévisibilité ou friction liée à la cyber-conflictualité. Les aléas techniques d'abord : les outils employés ne fonctionnent pas comme ils le devraient, rappelant que le cyberespace est un espace technique créé par l'homme. Les aléas stratégiques ensuite : une erreur de cible, de mode d'action ou de correspondance entre les deux entraine l'échec. Le cyberespace étant un domaine relativement récent où les stratégies sont peu codifiées et souvent empiriques, il est particulièrement imprévisible. Enfin les aléas temporels : le choix d'une action déclenchée à un instant se heurte ensuite à un événement de plus grande ampleur ou une modification inattendue annule le bénéfice de l'action. À la manière de ce que N. Taleb nomme « l'extrémistan », le cyberespace semble se développer comme le lieu même de l'imprévisibilité.

I Aléa technique

En tant qu'artefact, le cyberespace est soumis aux lois de la technique. En ce sens, le niveau de compétence technique des agresseurs et des victimes ainsi que le degré de diffusion des systèmes visés déterminent les effets finaux. Le choix de toucher tel système par tel moyen révèle outre la capacité de l'agresseur, sa volonté d'obtenir une diffusion large ou restreinte.

Le conflit mobilise des cyber-armes adaptées à une cible *via* une fonctionnalité ou une vulnérabilité particulière. En l'état, il n'existe pas de cyber-armes absolues efficaces sur l'ensemble du cyberespace, bien que certaines aient un spectre d'action plus large que d'autres comme le maliciel Conficker. En choisissant les systèmes Microsoft particulièrement répandus, Conficker dispose ainsi d'un champ d'action large à la fois géographiquement et par la variété des cibles touchées, nombre d'entreprises et d'institutions militairesutilisant des technologies duales fondées sur les systèmes Microsoft.

Le facteur humain détermine l'aléa technique : la compétence des agresseurs comme celle des défenseurs jouent sur l'imprévisibilité des résultats. Shamoon n'a rempli qu'une partie de sa mission. Certains éléments de son code laissent à penser qu'en plus de l'infection, de l'effacement de disque et du défacement de l'ordinateur avec un drapeau américain en feu,

celui-ci devait se connecter à un serveur distant. Or le module de connexion était inopérant, indice pour Kaspersky du faible niveau de compétence de ses concepteurs.

Shamoon montre aussi que tout élément technique utilisé contre un adversaire peut être récupéré par ce dernier. Cet élément, en conjonction avec d'autres, a orienté les analystes sur la piste de l'Iran. Le virus aurait été conçu à partir du *reverse engineering* de divers maliciels par un groupe d'une compétence technique somme toute limitée. Si le résultat n'a pas été à la hauteur des intentions, Shamoon s'est révélé particulièrement efficace pour paralyser les systèmes de décision et de communication de la Saudi Aramco durant plusieurs semaines.

L'aléa technique joue également sur le niveau d'interconnexion de la cible. En effet, une explication probable de l'absence de cyberactions lors des interventions militaires en Libye ou au Mali tiendrait au très faible taux de connexion de ces pays et au défaut de cible intéressante dans ce domaine. Si le cyberespace tend à devenir de plus en plus international, il n'en est pas encore devenu universel et incontournable.

II Aléa stratégique

La question de l'aléa stratégique renvoie à l'adéquation entre le mode d'action retenu et la cible. Si le cyberespace reste un espace technique, c'est aussi un espace stratégique où s'appliquent les règles classiques, même de manière inédite. La réaction imprévue de la cible ou de l'opinion renforce le brouillard de guerre, qui croît avec le nombre des opérations dans le cyberespace.

La première imprévisibilité stratégique tient à l'organisation même des agresseurs et des cibles. Selon ces facteurs, le niveau de succès variera et des opérations qui auraient pu être anodines prendront une ampleur insoupçonnée. Conficker a ainsi profité de la complexité propre aux chaînes de réaction cyber des entreprises et des organisations étatiques rigides comme les armées pour avoir un impact bien plus important que chez les particuliers. Si les individus effectuent de manière autonome et, pour une grande partie, automatique les mises à jour de sécurité de leurs appareils, les organisations sont soumises à des politiques globales et strictes en la matière. Le temps que l'information parvienne au décideur et que celui-ci la traite et répercute son choix sur la hiérarchie jusqu'à l'installation du patch correctif, le maliciel a eu le temps de se propager. Le correctif de la faille était publié par Microsoft avant même l'apparition du maliciel (23 octobre 2009 pour le patch, 21 novembre pour la

découverte de Conficker A) et seules des politiques rigides de cybersécurité, poussées à l'extrême expliquent qu'il ait pu se propager dans les systèmes militaires américains, britanniques et français.

A contrario, la mauvaise identification des cibles ou des relais transforme une opération en théorie viable en fiasco complet. Le cas OpGabon est significatif. Opération montée par les Anonymous contre les « meurtres rituels » pratiqués au Gabon, celle-ci vise à alerter l'opinion. Toutefois la faiblesse de couverture Internet locale combinée au désintéressement global pour la question en ont fait un échec patent. Plus encore, l'erreur d'appréciation de la situation locale a fait que certaines actions suivant l'opération en ligne (manifestations *in situ* par exemple) ont été récupérées par ceux-là mêmes qui étaient visés. L'inadéquation du mode d'action et de la cible représente un cas d'aléa stratégique majeur.

La faiblesse du maillon humain peut aussi avoir un effet stratégique. L'affaire PRISM et ses dérivés l'illustrent. Leur révélation, inattendue, résulte du choix fait par E. Snowden de révéler une pratique qui heurtait sa conscience, mais auquel participaient des milliers de personnes. Le scandale qui s'ensuivit ne tient ni à la technique, ni à une erreur d'exécution mais à une démarche venue de l'intérieur. Il est vrai que, sur des milliers d'employés d'une bureaucratie aux énormes archives, on peut s'attendre « statistiquement » à ce qu'il y en ait un qui trahisse ou fasse défaut.

La fiabilité humaine, au sein des grandes organisations devient une source majeure d'imprévisibilité. Les opérations les plus sensibles et les plus secrètes deviennent imprévisibles à mesure de l'augmentation du nombre de personnes impliquées. Il s'en suit un modèle contre-intuitif où l'avantage des États ou des grandes organisations est contrebalancé par l'imprévisibilité de leur personnel. Pour Stuxnet, une faiblesse humaine – supposément un sous-traitant connectant une clé USB dans un système d'information du centre de Natanz lui-même non-relié à l'Internet – entraîne la dispersion du ver dans le cyberespace en mars-avril 2010.

III Aléa temporel

Le choix de la temporalité est primordial pour toute cyber-action. Il peut être remis en cause par l'imprévisibilité d'événements ultérieurs.

Le cas Conficker illustre cette problématique puisque c'est Microsoft qui communique l'existence de la faille MS 08-67 au moment de la sortie du patch correctif en octobre 2009, le

maliciel n'apparaissant qu'un mois plus tard. Cela laisserait supposer qu'il a été créé grâce à la révélation de cette faille. En ce cas, Conficker ne serait pas une menace de niveau IV – découverte d'une nouvelle faille puis son exploitation par un groupe protéiforme et bien organisé - comme l'explique le DoD, mais plutôt de niveau II – utilisation d'une faille connue pour créer un nouveau virus. De là l'embarras des autorités militaires occidentales incapables de faire-face.

L'imprévisibilité dans le temps peut aussi tenir à la dispersion plus large que prévue de certains éléments qui se révèlent des menaces récurrentes. Des maliciels comme Ghostnet ont continué d'être actifs après avoir accompli leur mission initiale. La récurrence de ces éléments disséminés sur Internet intentionnellement ou fortuitement implique aussi de l'imprévisibilité. Le cas de Shamoon montre comment un virus sensé cibler Aramco s'est répandu dans d'autres systèmes comme RasGas, filiale commune ExxonMobil – Qatargas.

Chapitre 12 - Choix du discours et rhétorique stratégique

La guerre est une manière de convaincre l'adversaire qu'il a perdu. « La guerre n'est pas une discipline en soi, mais une sophistique armée (le prolongement de l'art d'avoir raison par d'autres moyens) » rappelle Peter Sloterdijk[136]. Durant les cyberconflits aussi les protagonistes « s'expriment » et luttent par des messages qui accompagnent l'attaque (ou qu'elle délivre implicitement), mais aussi pour convaincre des publics cibles. Autant de composantes cruciales de la cyberstratégie générale.

Nous distinguerons les figures du discours pendant des cyberconflits des discours relatifs au cyberconflit.

I Le discours pendant les cyberconflits

Partant de l'hypothèse que des messages qui accompagnent une cyberattaque visent à des effets psychologiques (faire peur, démoraliser, pousser à la faute, désigner à la vindicte, etc..) ou qu'ils doivent persuader (convaincre des tiers de la justesse de ses thèses ou de combattre un discours adverse), il faut s'attendre à y retrouver des fondamentaux, dont ceux de la rhétorique[137] (entendue ici comme l'art de gagner avec des mots voire des images). Mais il faut aussi s'attendre à rencontrer des spécificités liées aux particularités stratégiques et techniques de ces attaques. Un Etat ne tient pas le même discours quand il envoie des maliciels ou des B-52 (même si tous les langages martiaux puisent dans un fond commun que l'on peut faire remonter à l'Antiquité).

11 La rhétorique

La rhétorique classique combine des figures de langage bien répertoriées, les tropes, sensées agir dans le domaine :

- Du *pathos*, l'émotion. Il s'agit d'affecter pour convaincre. Ainsi créer des sentiments de peur ou d'admiration qui faciliteront l'adhésion à ce que l'on décrit comme vrai ou juste. *Nous avons subi une attaque, la prochaine pourrait être un Pearl Harbour informatique, il faut me donner les pouvoirs pour vous protéger*.

[136] Sloterdjik Peter, *Colère et temps*, éditions Maren Sell, 2007

[137] Au sens strict où, par exemple, Roland Barthes décrypte la publicité moderne en transposant le vocabulaire et les notions de la rhétorique aristotélicienne, ses tropes et figures, etc. Voir Barthes Roland, *L'ancienne rhétorique* (Aide-mémoire). In Communications, 16, 1970, Recherches rhétoriques pp. 172-223

• Du *logos*, du raisonnement logique qui amène l'interlocuteur aux conclusions souhaitées s'il adhère à certaines propositions et suit les conclusions que vous en tirez. Pour convaincre A de la culpabilité de B, on dira : *il avait le motif, la capacité et l'occasion, il a déjà été soupçonné dans des affaires similaires, donc c'est lui.*

• De l'*ethos*, l'appel aux valeurs auxquelles se réfère l'interlocuteur pour l'amener à juger que les thèses que l'on expose sont conformes à ses convictions. Ainsi : *si l'on croit aux principes généraux du droit international, il faut établir une législation des cyberconflits qui respectera les souverainetés des Nations*.

La rhétorique, recherche de ce qui est propre à persuader, enseigne comment composer des discours vraisemblables - qui semblent correspondre à la réalité mais ne portent peut-être que sur ce qui pourrait être- capables d'emporter la conviction. Ce glissement de l'hypothétique ou au crédible, s'applique aux textes sur la cyberstratégie. Ils visent souvent à convaincre soit que l'agression a été menée par le pays A dans le but X, soit qu'il convient de prendre certaines mesures pour éviter de telles agressions dont on décrit les effets probables et les remèdes adéquats. Nombre de figures de l'éloquence accusatoire se transposent sans trop de mal dans le débat sur le cyberconflit : argument d'autorité (*nos experts savent que...*), argument dit *ad personam* (*le caractère politiquement condamnable des dirigeants de ce pays démontrent leur culpabilité*), argument de vraisemblance (*une telle agression n'a pu être menée sans des moyens étatiques*), argument *ad consequentiam* (*si nous admettions ce que disent nos adversaires, nous irions vers la fin d'un Internet libre*.)... De même que la cyberstatégie ressemble par certains aspects à une enquête criminelle (qui l'a fait ?), la désignation et la vitupération du coupable présumé y tiennent une grande place[138].

12 La propagande

De la même façon, les grilles d'analyse de la propagande (qui n'est jamais qu'une rhétorique unilatérale appliquée aux masses) connues dès l'entre-deux guerres s'appliquent bien au cyber.

[138] On notera en retour qu'il existe des logiciels dits « rhétoriques » sensés aider à argumenter plus efficacement et que cela ne date pas d'hier. Nous en signalions l'existence dans Panoramiques n°52 (2° trimestre 2001), notamment les projets développés à l'époque par Thomson CSF Communications (projets dits Isocrate, Shopenauer, Perelman, etc.) p.82.

Ainsi, pour reprendre les catégories analysées dans les années 1930 par l'Institute for Propaganda Analysis[139] il ne serait pas très difficile de retrouver des techniques de :

- désignation (*name-calling*) et instrumentalisation du vocabulaire, comme dans l'emploi des termes agression, défense, terrorisme, guerre, surtout précédés de l'inévitable préfixe cyber ;
- transfert de valeurs associées à des notions, des institutions ou des expériences historiques (le « Pearl Harbour électronique » par exemple) ;
- arguments d'autorité, avec ici l'évocation des inévitables agences d'experts ou think tanks;
- appel au sens commun ou à l'unanimité, la communauté des internautes étant souvent présentée comme partageant les mêmes jugements ;
- recours à la peur, la crainte de la grande paralysie ou du grand accident informatique qui nous priverait des services les plus indispensables ;
- syllogismes, attribuant par exemple la culpabilité de certaines agressions à des pays parce qu'ils sont autoritaires ou auraient les moyens de mener de telles opérations ;
- extrapolations, telle l'évocation de « ce qui se passerait demain si un virus... ».

Outre ces techniques idéologiques, éristiques et polémiques très générales que nous pourrions qualifier de classiques, les textes relatifs au cyberespace présentent quand même des différences par rapport à l'éternel discours de l'hostilité.

Ils sont souvent marqués par le caractère spéculatif de tout propos sur un conflit dont les tenants et aboutissants restent incertains. Les problématiques du risque et de la culpabilité nourrissent des échanges basées sur des références techniques. Le tout, bien entendu, sur fond d'appel à l'autorité de la science, à la fois dans les pouvoirs de la technique, et aux lois de la modernité.

[139] Textes toujours mis en ligne par des successeurs de l'IPA et que l'on retrouvera sur des sites comme http://propagandacritic.com

13 La revendication

Il existe un « genre » de proclamation vengeresse et triomphante : le communiqué de revendication. Il sert à expliquer pourquoi l'on frappe pendant que l'on frappe (et qui peut, bien entendu, n'être ni authentique ni véridique).

Revendication et révélation

Cette pratique ne fait guère sens en cas d'espionnage. Signer ou signaler le vol clandestin d'un secret semble illogique. Mais il n'est pas rare de voir l'agresseur « sous-titrer » des actions de sabotages, ou *a fortiori*, des actes de subversion. Cela semble presque systématiquement le cas pour des groupes activistes de type Anonymous ou LulzSec. Cela paraît cohérent : interpeller, dénoncer, ou mettre au pilori États ou entreprises coupables (d'une atteinte aux droits de l'homme, par exemple) font partie des objectifs de ces groupes. Ils ne négligent jamais la pédagogie de leurs actes. Et comment mieux le faire qu'en taguant la sentence sur le site adverse ou en publiant des preuves de ses infamies - comme des documents compromettants qu'il dissimulait ou des vidéos ravageuses - ?

L'idée de châtier et démontrer est comme consubstantielle à ce projet. Les abus de pouvoir, réels ou supposés, sont donc « punis » par l'arme de l'information (numérique et verbale) et le dommage (site défiguré ou bloqué quelques heures, archives secrètes mises en ligne) importe moins que la publicité faite à l'exploit des bons et à la défaite des méchants. Cette double logique - publier les crimes de l'adversaire et lui adresser un message de défi - suppose au moins une ébauche de justification de l'action.

Certains théorisent la chose. Ainsi Julian Assange développe une thèse simple mais frappante[140] : les gouvernants élus pour servir le Bien commun le trahissent et détournent le pouvoir à leur profit, donc ils complotent, donc ils échangent beaucoup de documents, donc nous, hackers, pouvons nous emparer de ces documents et les révéler au peuple, donc plus la conspiration est importante et complexe, plus elle est fragile.

Dans un autre style, les Anonymous reprennent un message récurrent et nourris de clins d'œil à la culture pop avec ses super-héros et ses vengeurs masqués. Le fond est simple, plutôt emphatique et lyrique « Nous sommes les Anonymous. Nous sommes légion. Nous ne pardonnons pas... », ou « Les corrompus nous craignent. Les honnêtes nous soutiennent. Les

[140] Assange Julien, *La conspiration comme mode de gouvernance*, 2006 disponible sur http://www.contretemps.eu/interventions/art-fuite-philosophie-politique-julian-assange-par-lui-meme

courageux nous rejoignent », le tout adapté en fonction du gouvernement ou de l'organisation cible.

D'autres agressions, inspirées par d'autres idéologies, se prêtent à des messages simples et courts. Ceux de l'Armée électronique syrienne (AES) tournent presque systématiquement autour de trois thèmes : nous avons accompli un exploit, nous soutenons Bachar, nos ennemis sont des menteurs... Cela n'appelle guère d'analyses doctrinales.

Les messages sont souvent d'un « moralisme » désarmant, manichéens. Ainsi, lorsque l'AES s'en prend à Forbes, elle prend soin de préciser qu'il s'agit d'un châtiment mérité et non d'une démonstration gratuite : « @Official_SEA16: We didn't publish the user table of Forbes to show off, but because they deserved to be embarrassed. #SEA ».

Autre exemple avec « l'Epée Tranchante de la Justice » qui, parallèlement à l'agression Shamoon, a posté de façon anonyme sur Pastebin. « Nous agissons au nom du groupe de hacker anti-oppression, révolté par les crimes et atrocités qui se déroulent dans divers pays voisins, tels que la Syrie, le Barhein, le Yémen, le Liban, l'Égypte... et par le deux poids deux mesures appliqué par la communauté internationale à ces pays. Nous avons donc voulu frapper par notre action les principaux responsables de ce désastre. Un des principaux est le régime corrompu d'Arabie saoudite qui finance ces crimes en utilisant les réserves de pétrole des musulmans... » Sauf peut-être la très vague indication que tout cela a été financé avec le pétrole des musulmans (*by using Muslims oil ressources*), c'est un acte d'accusation assez vague contre Riyad et un tel manifeste aurait pu être signé par un très vaste éventail politique. Il faut beaucoup interpréter - surtout évoquer la question : « à qui profite le crime ? » - pour voir là une responsabilité iranienne ou shiite. Après les arguments techniques sur la « filiation » du virus, les arguments sémantiques ou politiques extraits des communiqués laissent les interprétations ouvertes.

Le cas terroriste

Les terroristes, depuis la fin du XIX^{e} siècle, frappent toujours une cible symbolique[141] (un représentant de l'ordre, un « occupant », un ennemi idéologique, voire un passant qui représente une certaine religion ou une certaine nationalité). Mais ces intellectuels d'encre et

[141] Une anthologie de textes sur « Terrorisme, médias et communication » est disponible (29 mai 2014) sur http://Huyghe.fr/actu_227.htm). Voir également A. Bauer et F.B. Huyghe, *Les terroristes disent toujours ce qu'ils vont faire,* PUF, 2008.

de poudre ajoutent souvent à la mise en scène de l'action[142], la pédagogie du texte puis de la vidéo. Combinant ravage de l'attentat et le message des revendications, ils font un mélange de publicité et de pédagogie à travers des proclamations successivement écrites, puis téléphonées et maintenant mises en ligne. Notre propos n'est pas d'assimiler toute cyberagression à un crime terroriste, mais de rappeler qu'une même logique - donner du sens à un acte qui se veut exemplaire - peut se retrouver dans les deux cas.

Le communiqué de revendication est une longue tradition qui remonte aux années 1880. Ce genre combine toujours peu ou prou les mêmes rubriques : l'auteur, son idéologie et la cause qu'il défend, sa cible et le crime qui lui vaut d'être frappée, qui elle représente, les revendications, la promesse de combats plus durs ensemble pour l'avenir et jusqu'à la victoire finale. Dans le monde des cyberagressions, ce « sous-titre » remplit à peu près les mêmes fonctions, mais il est souvent d'un simplisme dont on ne sait trop s'il tient au niveau idéologique des agresseurs ou aux contraintes du vecteur technologique employé : quelques slogans sur une page d'accueil remplacent des dizaines de feuillets comme en écrivaient les activistes des années de plomb.

II Les discours au sujet des cyberconflits

La perspective change si l'on s'intéresse non plus au discours qui accompagne les agressions, mais aux locuteurs « officiels » ou experts traitant de cyberguerre et thèmes assimilés. Il n'est pas possible, bien entendu, de résumer les milliers de pages produites sur la cybersécurité ou la cyberdéfense. Mais on peut au moins signaler des thèmes récurrents.

La dramatisation du danger

Le premier renvoie à la notion du danger ; il fonctionne souvent en comparant les effets virtuels d'une agression à des catastrophes déjà connues. Un Waterloo informatique ou un Pearl Harbour électronique, deux mantras du discours alarmiste américain[143], en sont des exemples. Cybergeddon, néologisme qui réunit le préfixe cyber et la référence biblique à Armageddon donne des connotations apocalyptiques à la perspective du *Big one*, la grande

[142] Voir Cahiers de Médiologie n° 13, *La scène terroriste,* Gallimard 2002.
[143] Des auteurs comme Winn Schwartau, ancien directeur du *Manhattan Cyber Project*, produisent sur ce sujet litérallement depuis des décennies.

agression qui ferait s'effondrer une structure technologique omniprésente. Un nouveau vocable est apparu dans les publications de l'OTAN : Pandémonium.

Dans un registre plus sobre, mentionnons la métaphore de la catastrophe naturelle (par exemple le Secrétaire d'État L. Panetta comparant une future agression contre des infrastructures vitales à un ouragan, mais « en pire »).

Le thème de la dépendance technologique

Autre procédé : faire peur en s'appuyant sur l'argument (pas totalement absurde) selon lequel la fragilité des sociétés technologiquement avancées est proportionnelle à leur dépendance à l'égard de dispositifs numériques servant à stocker, faire circuler, traiter l'information, opérer des transactions, etc.

Des discours et rapports décrivent le résultat d'agressions contre des infrastructures vitales ou sensibles de façon assez dramatique. La crédibilité des scénarios est souvent renforcée par des exercices de simulation (sorte de *kriegspiels* destinés à tester la cybersécurité) ; leurs résultats se révèlent régulièrement très alarmants.

L'argument de la catastrophe en chaîne est souvent employé par des sociétés qui ont quelque chose à vendre, solutions commerciales de sécurité ou budgets de leur service, ou par ceux qui sollicitent une aide internationale. Se félicitant que « cette fois-ci » le dommage ait été limité par une solide défense et par une résilience assez rapide, les victimes noircissent le tableau de la prochaine agression qui pourrait bien être fatale. Tous ont intérêt à rendre plus redoutable encore le péril. Cela n'implique pas, bien entendu, qu'il soit inexistant.

Le thème des comparaisons historiques

Des thèmes comme le « nouveau Yalta[144] » (à propos de la réunion de l'UIT de Dubaï en décembre 2012), le cinquième et nouvel espace où s'étendrait le conflit, la nouvelle dissuasion, les nouvelles lignes rouges à ne pas franchir, sans oublier l'inévitable nouveau onze septembre cyber, etc. sont très courantes. Elles traduisent un effort pour ramener des phénomènes inédits à des catégories familières, notamment dans le raisonnement stratégique. Tantôt ce sont des comparaisons avec la logique de la Guerre froide ou de la Guerre des étoiles. Tantôt la grande agression cyber est présentée comme la répétition traumatique d'une

[144] Center for New American Security, *A New Yalta*, 2013, http://www.cnas.org/files/documents/publications/CNAS_WCIT_commentary.pdf, accessible le 29 mai 2014.

expérience terrible (le 11 septembre par exemple, comme le faisait souvent l'ancien cyber-tsar, Richard Clarke)... mais multipliée par la puissance du numérique et des réseaux.

Le discours de la peur se nourrit aussi des jeux de sens portant sur les catégories : le crime, la guerre, sécurité, le terrorisme (avec l'inévitable préfixe cyber)...

Le choix des mots

La question de la qualification (« acte de guerre » par exemple), outre ses implications juridiques strictes, joue un rôle psychologique. Le mot guerre fait peur : les responsables américains se disent soucieux de ne pas risquer la sécurité des civils ou de faire quoi que ce soit qui évoquerait un crime de guerre. Les références au *jus ad bellum* - la capacité des Etats-Unis de riposter par des armes classiques à des agressions cybernétiques d'une certaine gravité ou au *jus in bello* - refus de faire des victimes civiles, en utilisant leur propres cyberarmes – sont fréquentes. Depuis l'annonce par les chercheurs de la Rand en 1993, *Cyberwar is coming*, l'hypothèse donne lieu à force effets d'annonce.

Les adversaires du laxisme sémantique s'élèvent contre l'abus du mot (l'exagération, le *hype* disent les auteurs anglo-saxons). Leur critique s'appuie sur des raisons de fond - l'essence de la guerre suppose la létalité des agressions (pas de guerre sans morts), leur publicité (des acteurs bien identifiés, si possible des États, s'affrontant autour d'un différend connu), le caractère politique des buts poursuivis (qui implique à son tour le caractère instrumental de la dimension purement militaire), la paix comme fin durable de la guerre, l'enchaînement des offensives et contre-offensives sous la forme du duel clausewitzien, et non par une seule agression éphémère.

Des auteurs comme Thomas Rid soutiennent que la « cyberguerre n'aura pas lieu » avec des arguments purement stratégiques. Ils concède qu'il y aura certainement des cyberagressions, prédation par ordinateurs interposés et utilisation d'adjuvants cyber dans le cadre de conflits plus classiques. Mais, pour des raisons tenant au calcul rationnel, au contrôle de l'instrument, des moyens et des effets, une cyberguerre à titre « principal » paraît trop aléatoire pour se développer selon la logique de la montée aux extrêmes.

Cela ne contredit pas le fait que des opérations militaires ou leur menace soient de plus en plus accompagnés d'actes de malveillance numériques, ni que ces derniers ne tendent à se multiplier.

Parmi les arguments les plus débattus, l'ignorance où est la victime de l'identité certaine de l'agresseur et de sa capacité est souvent présentée comme incompatible avec la notion de guerre (ce qui revient à la notion de non publicité que nous évoquions plus haut). Mais certains, comme Eugene Kaspersky dont l'entreprise a découvert le virus Flame, en déduisent que le terme plus adapté serait cyberterrorisme.

Le cyberterrorisme

Le cyberterrorisme[145] est également un bon exemple de ces glissements sémantiques par contamination. L'horreur suscitée par le poseur de bombes ou le tueur d'innocents se reporte sur des activités qu'il serait plus exact de qualifier de subversives ou protestataires et qui n'ont, *a priori* ,tué personne jusqu'à ce jour. Utilisé dès les années 1990, par exemple par Win Schwartau[146], discuté depuis plus de dix ans, le terme « cyberterrorisme » a connu un succès lié à toutes les connotations qui s'y attachent, et joue sur l'idée que les vulnérabilités de nos systèmes interconnectés seront forcément exploitées par des groupes privés à motivations idéologiques. La cyberconflictualité porterait à son paroxysme la logique de l'asymétrie. Par ailleurs, une importante littérature s'est emparée du thème éminemment romanesque de l'organisation cachée dans l'ombre mettant à genoux une puissance politique grâce à quelques virus habilement répandus.

L'usage de « terrorisme » disqualifie le coupable présumé, par exemple le fait de nommer « cyberterrrorisme » des agressions contre l'Estonie en 2007, qui consistaient surtout en dénis d'accès. Il est vrai que des dénis d'accès visant par exemple les systèmes d'information des organismes de secours peuvent les empêcher d'intervenir et donc entraîner des dommages aux biens et aux personnes. Les références à une menace « invisible » et à un risque pour des victimes « innocentes » jouent aussi.

Certains acteurs politiques peuvent choisir de dénoncer les maux qui sévissent sur Internet, glisser de la stigmatisation de la piraterie à celle de la désinformation et des discours de haine, et à l'évocation de la pédophilie, de la pornographie et de divers trafics, pour finir par dénoncer des discours sectaires ou antinationaux, le tout regroupé sous la même catégorie que la cyberpiraterie et le terrorisme. Ces amalgames finissent par englober toute forme de dissidence ou opposition en ligne. Tel pays qui censure sa cyberdissidençe peut ainsi se placer sous le drapeau de la lutte contre le Mal. Pourtant, de faire pénétrer un virus à faire pénétrer

[145] Voir O. Kempf, « Cyberterrorisme, un discours plus qu'une réalité », *Hérodote*, printemps 2014.
[146] Voir Win Schwartau in L*'information, c'est la guerre,* Panoramiques, 2001, PP. 101-106

une idée, il y a des différences qu'il n'est pas innocent de gommer et cela devrait nous mettre en garde contre ces phraséologies.

Chapitre 13 - Influence

Toute cyberagression suppose une intention hostile, *a minima* une malveillance (comme en témoigne l'expression « logiciel malicieux »). Que l'agresseur s'efforce de diminuer les capacités de la victime, en lui dérobant un savoir, en l'empêchant d'utiliser ses moyens ou encore en l'offensant avec des mots et des images, elle subit un dommage. Certains effets se réalisent dans l'ordre de la puissance : les gains et pertes se mesurent alors par un différentiel de capacités économiques, technologiques, militaires. Il s'apprécie par comparaison avant/après : le pays A s'est emparé d'éléments du patrimoine informationnel du pays B, provoqué le chaos dans ses systèmes de contrôle et de régulation (pendant que A avance ses pions sur l'échiquier militaire, diplomatique ou autre, car sinon, à quoi bon avertir l'autre du mal qu'on peut lui faire ?).

D'autres effets des cyberagressions relèvent de l'influence[147] : ils agissent sur la décision ou les éléments de jugement d'autrui (« victime » ou tiers), de façon positive ou négative.

I Influence positive

11 Caractéristiques

L'influence se mesure à la probabilité que celui qui la subit se conduise ou juge comme le désire l'influent sans qu'il ait à exercer de contrainte à son égard, ni à verser de contrepartie. L'influence est souvent associée à des notions positives comme le prestige (qui joue sur le besoin d'imiter), la séduction, la persuasion et d'autres relations où l'image ou le message le plus souvent produits délibérément (on peut influencer sans le vouloir) incitent à approuver ou à se conduire de la façon désirée. Ainsi, la notion de *soft power* reflète ce rapport multiforme : possède du *soft power* le pays qui reçoit des soutiens dans les assemblées internationales, dont les autres peuples apprécient hautement la culture, les performances sportives, les personnalités phares, dont le mode de vie jouit d'une certaine attractivité, dont l'idéologie se répand hors de ses frontières, qui présente une bonne image, qui est connu pour une attitude amicale, ouverte à la coopération dans les relations internationales, et d'autres traits qu'il

[147] Pour notre analyse des techniques et organisations d'influence, voir F.B. Huyghe, *Maîtres du faire croire. De la propagande à l'influence*, Vuibert, 2008.

semble aussi désirable de posséder que difficiles à produire délibérément. Depuis des siècles l'État emploi des techniques d'influence, allant de la politique de prestige jusqu'aux formes modernes du *storytelling* ou du *branding*). Celle-ci se répand aussi à travers des organisations qui n'exercent pas d'autorité politique, n'emploient pas la violence, ne cherchent pas le profit, mais qui suggèrent aux décideurs ou à l'opinion des idées, des croyances et attitudes, des choix et préférences. Nous incluons dans cette catégorie les ONG, les lobbies, les think tanks, mais aussi les médias, les réseaux sociaux voués à la discussion et à l'évaluation.

Pour simplifier, nous appellerons « positive » l'influence qui vise à rallier des partisans ou à faire partager un point de vue.

Par point de vue, il faut comprendre aussi bien l'interprétation d'une situation concrète que des habitudes mentales, un mode de management ou un système juridique, voire une idéologie, des valeurs, des références culturelles, et plus largement encore tout ce qui pousse à juger comme le souhaite ceux qui exercent l'influence. Ceci peut se pratiquer directement et ouvertement ou indirectement comme à travers des organisations relais, qui n'affichent pas toujours leur appartenance. Le message reste clairement positif et porte sur des choses décrites comme vraies, souhaitables ou morales.

12 Mise en œuvre dans le cyberespace

Une influence de ce type s'exerce-t-elle sur Internet ? La réponse est évidemment oui : la plupart des messages que nous recevons - ne serait-ce qu'un simple *like* ou une recommandation - visent à nous persuader qu'il est souhaitable de : voter, acheter, adopter telle position, admirer ou visiter untel.... Il est difficile de dresser la liste des méthodes, souvent désignées par des anglicismes et qui sont sensées produire de l'influence sur Internet : *marketing* politique, *branding, public affairs, storytelling, perception management, e-influence, e-réputation, buzz* positif, *community managemen*t, *slacktivism*[148]... Toutes ces méthodes doivent exercer une influence sur des acheteurs, des électeurs, des décideurs et leaders d'opinion, des alliés, des neutres, etc. Certaines sont plus que suspectes. Il est même possible de simuler des courants d'opinion[149] en achetant ou en produisant de faux partisans

[148] Pour le sens de cette terminologie,, nous renverrons au glossaire de 500 mots que nous avons mis en place sur http://Influcrise.wordpress.com (consulté le 29 mai 2014).
[149] Cette technique est souvent désignée par l'anglicisme *Astro turfing*, du nom d'une marque de gazon artificiel.

en ligne. Nous nous limiterons ici à étudier la stratégie à partir des notions de victoire et d'adversaire.

Que des actions d'influence positive puissent se déployer dans le cyberespace, voilà qui n'a pas échappé aux décideurs dont beaucoup se persuadent volontiers qu'il faut investir les réseaux sociaux. Des professionnels, qu'ils soient *spin doctors* ou spécialistes des logiciels cartographiant les *e-influents,* prospèrent grâce à cette tendance ou à cette mode.

13 Modes d'influence propres au cyberespace

Deux traits des luttes d'influence dans le cyberespace semblent particulièrement remarquables et qui tiennent moins à la nature du message (l'énoncé auquel s'appliquent les règles rhétoriques évoquées précédemment) qu'aux conditions de son énonciation et de sa circulation. Nous les nommerons contagion communautaire et lutte pour l'attention.

131 Contagion et communication

La contagion communautaire ne ressemble plus guère à la propagande de masse, un message standardisé adressé par des spécialistes à des foules passives. Elle se concilie mal avec les médias traditionnels, le journal, la radio ou la télévision, fonctionnant selon un schéma « un vers tous » : en dépit de tentatives pour donner la parole à l'audience et l'impliquer (p.e. ce qu'Umberto Eco appelait la « neo TV »[150]), l'émetteur dans les *mass media* propage un message élaboré avec des outils sophistiqués et coûteux, destiné à un public vaste, dispersé et souvent indistinct. L'efficacité de ce message dépend de sa force persuasive ou attractive, de son adaptation aux mentalités des audiences, de la puissance de ses vecteurs (d'où la compétition des télévisions par satellite pour influencer hors de ses frontières) et de la façon dont son contenu est reçu par des leaders d'opinion ou des médiateurs.

Après plusieurs décennies de travaux sur « Internet sensé rendre chacun émetteur à son tour », sur le projet de « ne plus haïr les médias, mais devenir les médias », sur la diffusion de l'information qui échapperait à toute censure et sur les technologies numériques, sur les « foules intelligentes », il n'est pas question de nier que les dispositifs d'influence évoluent depuis une diffusion pyramidale via des relais d'opinion et à des filtres, celle des médias classiques, jusqu'à un nouveau modèle : une circulation / reconstruction / évaluation / signalisation des messages au sein de communautés rassemblées par des goûts, liens ou

[150] Umberto Eco, *La guerre du faux*, chapitre "Neo TV et archéo TV", Gallimard, 1967.

intérêts. Il importe alors bien moins de délivrer un message bien formaté à des destinataires dont le rôle se bornerait à acquiescer que de lancer un message contagieux. Cela implique que chaque membre des réseaux ait un motif de s'approprier, d'approuver ou enrichir et de vouloir le propager à son tour. Le lien qui unit ceux qui partagent compte souvent davantage que la force de conviction des discours et des images disponibles. On peut considérer ce lien comme « faible », lorsqu'il se réduit à une participation distraite et peu impliquante à des débats et partages sur des intérêts communs. Mais ce lien peut devenir fort, nourrir des passions collectives et transformer la bande de copains en ligne ou les *slacktivists*[151] vaguement indignés en une communauté soudée prête à descendre dans la rue[152]. Au « le médium, c'est le message », on peut désormais rajouter que le lien (d'appartenance, coopération, intelligence collective, etc.) est le message.

132 Guerre de l'attention

Le second facteur critique est la lutte pour l'attention. Partant du principe qu'il est de plus en plus difficile d'empêcher les récepteurs d'accéder à des opinions adverses ou à d'autres versions critiques, ou même délirantes, de la réalité, le but du jeu de l'influence devient d'attirer des flux dynamiques vers son message (sa page Facebook, son tweet, son lien, sa vidéo en ligne...). La réussite ne consiste plus à interdire à l'autre de s'exprimer ou à écraser son argumentation par une puissante dialectique, mais à submerger littéralement son discours sous les opinions contraires ou neutres, à le rendre le moins accessible par les moteurs de recherche, à en détourner les réseaux sociaux, à susciter une impression d'unanimité. Les nouvelles conditions du succès ont peu à voir avec les recettes servant à rédiger un éditorial ou à se préparer à un débat télévisé (*media training)* telles qu'elles se pratiquaient déjà il y a vingt ans. De l'art du référencement à celui de la gestion des communautés, de nouvelles disciplines apparaissent qui en tiennent compte.

14 Illustrations

Comme souvent les exemples les plus explicites (ou les plus commentés) proviennent des Etats-Unis, notamment l'évolution de la diplomatie publique.

[151] Désignation des activistes paresseux qui militent d'un clic de souris sans s'engager vraiment dans la vraie vie.
[152] Comme cela s'est vu lors du printemps arabe en Égypte et en Tunisie.

141 Diplomatie publique

Au départ, il s'agit typiquement d'une pratique de Guerre froide : s'appuyant sur une pratique antérieure (la guerre culturelle menée par la CIA), une agence américaine l'USIA (US Information Agency) créée en 1953 centralise la gestion de médias (de type *Voice of America* ou *Radio Free Europe*...) qui émettent au-delà du rideau de fer, mais aussi des réseaux humains d'amis des Etats-Unis, la distribution de produits culturels, écrits ou audiovisuels reflétant les valeurs occidentales, la gestion d'une stratégie d'image du pays. Il s'agit de plaider sans détour la cause américaine et de propager une idéologie suivant un plan centralisé de « croisade pour la liberté ».

Ces pratiques, mises en sommeil après la chute de l'URSS, retrouvent une nouvelle jeunesse à l'ère des réseaux sociaux. Il est maintenant question d'une « nouvelle diplomatie publique » pour combattre idéologiquement l'extrémisme violent (euphémisme pour jihadisme). Ces nouvelles pratiques sont à rapprocher des notions de e-diplomatie promue par Hillary Clinton ou de concepts produits par son maître à penser, le doyen Nye comme *Smart Power* ou *Cyber Power*.

La nouvelle diplomatie publique combinerait les pratiques de « l'ancienne », comme lancer des programmes culturels, des visites, des réseaux alliés), et une attention particulière apportée à la compréhension des autres cultures, à la mise en valeur de ses propres productions culturelles *mainstream*[153], au dialogue y compris avec l'adversaire, aux relais que constituent les ONG et think tanks (par exemple les associations financées par George Sorros). Et bien sûr, une énorme attention apportée aux réseaux sociaux.

Dans cette stratégie ces derniers sont à la fois :

- des lieux d'expression de l'ambassadeur qui tweete dans la langue du pays où il est en poste au simple G.I. incité, lui aussi, à donner une image positive de l'action américaine en opérations extérieures ;
- des sources de veille et d'observation de tendances, notamment à l'égard des Etats-Unis et de ses valeurs ;
- un terrain d'affrontement verbal avec les groupes adverses, p.e. pour dénoncer leur lâcheté (« vous tuez des femmes et des enfants ») ;

[153] Ce qui ne signifie pas que les productions culturelles qui plaisent à tous soient forcément *made in USA*, comme le démontre Frédéric Martel dans *Mainstream* (Flammarion, 2011).

- une manière de mobiliser ses propres communautés sympathisantes, comme les vétérans ou les familles de soldats qui contribueront à donner une image plus positive et plus humaine quitte à leur fournir documentation ou éléments de langage
- une vitrine pour les valeurs et le mode de vie américains ;
- un moyen de former, aider matériellement et techniquement, bref de soutenir les cyberdissidences et mouvements « démocratiques » qui gênent des pays autoritaires hostiles aux Etats-Unis suivant le schéma des printemps arabes ; voire un moyen d'embarrasser l'adversaire comme lorsque l'USAID subventionne un équivalent cubain de Twitter, partant du principe que, là où il y a des réseaux sociaux, la critique du régime se développe, voire que le nouveau médium technologique provoquera automatiquement des révoltes politiques[154] :
- une illustration du principe que plus s'étendent librement les technologies numériques, meilleur c'est politiquement, économiquement et idéologiquement bons pour la nation universelle par excellence, les Etats-Unis ;
- cette pratique n'est pas un monopole américain. Ainsi, l'armée britannique a une méthode d'influence stratégique où tous, du général au moindre quartier maître, doivent décliner un même « grand récit », y compris et surtout sur les réseaux 2.0.

142 Tsahal

Quant à la notion de guerre de l'attention, il est difficile de mieux l'illustrer que par les pratiques de Tsahal. Après plusieurs échecs en matière de communication face à ses adversaires, de l'opération Plomb durci, la Force de Défense Israélienne s'engagea dans la « guerre du *tweet* » (y compris en anglais et en français) contre le Hamas en novembre 2012. Il s'agissait de profiter de la nature « épidémique » typique d'une plate-forme de micro-blogging pour :

- attirer l'attention des médias classiques vers ses liens, ses images, ses sites plus vite que l'adversaire, rendre très accessible tout ce qui peut soutenir son argumentaire ;

[154] A noter qu'en l'occurrence la méthode ne se révèle pas très efficace : ces réseaux qui coûtent cher aux contribuables américains ont certes un certain succès de convivialité chez les Cubains, mais n'a guère de résultats politiques : il ne suffit de donner au citoyen un accès au Web 2.0 pour qu'ils se révoltent. Voir http://bigstory.ap.org/article/us-secretly-created-cuban-twitter-stir-unrest visité le 30 mai 2014

- décrédibiliser ledit adversaire en fournissant très vite des « preuves » de sa duplicité ou en pratiquant la métapropagande, méthode qui consiste à persuader que tout ce que dit l'adversaire ou ses partisans relève de la propagande et de la désinformation ;

- motiver sa « communauté », en l'occurrence fournir aux amis d'Israël des arguments, des images pour démontrer, par exemple, que Tsahal pratique des frappes chirurgicales, leur proposer des affiches de propagande, des sources où trouver chiffres ou exemples ;

- augmenter la visibilité de son propre matériel de propagande ou des sites amis (toujours le principe : plus il y a de *tweets* et de *like*, plus il y a de visiteurs, meilleur le référencement, plus fortes les chances que « votre » message parvienne aux médias et au public plutôt que celui de l'ennemi) ;

- de façon plus générale, offrir une bonne image de Tsahal, avec ses jeunes soldats enthousiastes et adeptes des nouvelles technologies.

Toutes les armées n'en font pas autant : elles peuvent être frileuses à l'égard des réseaux sociaux pour des motifs de sécurité (peur que des soldats ne laissent filtrer des informations confidentielles ou peur qu'ils ne se laissent aller sinon à des propos exploitables par une presse hostile). Mais aussi par réticente à l'égard de l'influence, par crainte d'être accusés de « faire de la propagande » ou « de l'idéologie ».

Un mouvement de fond porte les institutions, non seulement à être présentes sur les réseaux sociaux, mais aussi à en assumer la dimension d'influence. Celle-ci peut impliquer la défense de ses valeurs et principes donc le besoin de raconter un « récit principal » de justification. Comme pour toute communication persuasive, le problème est de vaincre trois obstacles qui sont d'abord le temps (instantanéité de diffusion et conservation des documents en ligne) et la distance (les autorités ne contrôlent plus guère le territoire lorsqu'il s'agit de la diffusion en ligne, sauf à se ranger dans les « ennemis d'Internet » et à y investir beaucoup d'efforts). Le troisième, contrairement aux deux premiers, ne peut être vaincu par la seule performance technologique : c'est la réticence du cerveau humain. L'objectif est de conquérir deux ressources : la confiance et l'attention, conditions indispensables à la bonne réception et acceptation du message. Il est probable que les institutions et même les armées, en dépit de

leurs hésitations[155] finiront pas s'engager dans l'influence en ligne, comme les grandes entreprises, avec ce que cela implique de controverses éventuelles.

143 Révoltes 2.0

De la même façon, si l'on a célébré un peu hâtivement une « révolution Facebook » ou une « révolte 2.0 » qui expliqueraient les printemps arabes, une autre tendance lourde pousse des groupes d'opposition vers les réseaux. Souvent non hiérarchisés, plus ou moins spontanés, sans idéologie très structurés ni leaders officiels, ces mouvements utilisent les réseaux sociaux pour une triple fonction[156] :

- expression de leurs critiques, de leurs revendications, de leurs appels à la mobilisation, de leurs thèmes (souvent négatifs : à bas Untel, halte à ceci) ;
- formation de communautés en ligne : des réseaux qui servaient initialement à échanger sur de vagues intérêts partagés ou des affinités s'enflamment : le groupe se soude de plus en plus autour de passions communes, y compris politiques, et évolue du lien « faible » qui unit les internautes (par écrans interposés) au lien fort des militants et des manifestants ;
- coordination stratégique au moment du passage à l'action amplification des mobilisations (y compris en nourrissant les médias classiques pour leur donner plus d'écho).

Des marques aux révolutions, la tendance à utiliser les réseaux sociaux comme outil de mobilisation des communautés d'affinités s'inscrit dans la durée.

II Influence négative

L'influence peut servir à pousser à la faute ou à la dissension, ruiner des réputations, susciter des contestations, priver d'appuis ou susciter des adversaires. Calomnier, désinformer, démoraliser, diviser, lancer des offensives psychologiques, dénoncer, ridiculiser, mais aussi publier des documents révélateurs, organiser une opposition ou des manifestations, autant de méthodes dont les résultats peuvent s'amplifier dans le cyberespace.

[155] Voir étude EPS 2011/74 « Les communications institutionnelles de la défense en Europe : comment les pays européens communiquent sur leurs armées » D. Chaize, F.B. Huyghe (dir.) F. Liberti, J-P Maulny, P. Migault, A. Tuaillon

[156] Analysée dans Médium n° 29 « Réseaux : après l'utopie », 2011, dirigé par L. Merzeau et F.B. Huyghe

21 Cyberagression et influence

Les cyberagressions présentent deux spécificités pour une stratégie d'influence négative :

- le rôle du secret. L'espionnage le présuppose (le vol d'information est un moyen d'augmenter ses capacités, pas son influence). Le sabotage est souvent anonyme (ou accompagné de signatures douteuses) et ses objectifs parfois cachés. Quant à la subversion, dont il est évident qu'elle relève de l'influence, elle se pratique souvent aussi en dissimulant une part des informations (par exemple l'identité des membres d'un réseau social pour échapper à la police).
- le rôle de la violence par l'information. Une cyberagression suppose au moins une violation : forcer un système de protection, s'emparer de privilèges indus dans le contrôle des machines, perturber un fonctionnement normal. Cette violence passe parfois par des opérations matérielles ou par le code qui agit sur les machines mais trouve toujours son sens dans la couche sémantique : espionner, c'est accéder à ce qui devrait vous être cachés, saboter, c'est empêcher l'adversaire de donner des ordres efficaces. Enfin, la subversion implique, outre l'efficacité du message, l'art d'imposer ses signes à la place de ceux de l'adversaire.

Ces deux éléments - agir masqué, et utiliser le code pour un dommage dans le monde sémantique et symbolique - favorisent les actions négatives.

22 Toucher l'image de la victime

La plupart des stratégies négatives attentent à l'image de leur victime soit directement, affectant le moral ou la cohérence d'un camp, soit indirectement en agissant sur les neutres ou les alliés[157].

Un dirigeant qui découvre que le site du ministère des Finances ne fonctionne pas, que le portrait du président s'est vu affubler des moustaches d'Hitler ou que des millions d'internautes les conspuent, peut, en effet, éprouver un dommage psychologique, moral ou de réputation. Donc une perte de sa propre influence. Mais l'effet sur l'opinion peut le toucher davantage.

[157] Même si, une fois encore, il y a plus d'un siècle que l'on incite des soldats ennemis à déserter (tracts sur le thème « Votre guerre est inutile et vos chefs se moquent de vous ») ou que l'on persuade l'opinion internationale que le belligérant X commet crimes sur crimes (*atrocity propaganda*).

L'effet mesurable (tel site bloqué tant d'heures, tant d'internautes qui ont repris le slogan « dégage », tant de documents compromettants publiés) n'a de sens que par son effet sémantique et par la publicité qui l'entoure.

Du ridicule

Parmi les facteurs qui concourent à ce résultat, le sentiment de ridicule. Un gouvernement, une armée, une organisation importante sont vulnérables face à des techniques qui ressemblent parfois à des canulars d'étudiants ou à la pure dérision. Un exemple de la littérature des Anonymous s'en prenant à Sony : « Vous avez abusé du système judiciaire pour censurer les informations concernant le fonctionnement de vos produits. Vous avez agressé vos propres clients simplement parce qu'ils possédaient et partageaient ces infos. Ce faisant, vous avez violé la vie privée de milliers d'entre eux. Des informations qu'ils voulaient communiquer au monde gratuitement. Les mêmes que vous voulez détruire pour préserver l'avidité de votre société et asseoir définitivement votre contrôle sur les utilisateurs. Maintenant, vous allez connaître la colère des Anonymous. Vous avez vu un nid de frelons et y avez enfoui vos pénis. Vous devez subir les conséquences de vos actions, à la manière Anonymous »[158].

De l'humiliation

Dans un registre très proche, l'humiliation est d'autant plus forte qu'un État ou une puissante compagnie de type Aramco apparaissent désarmés face à l'ingéniosité technique d'un adversaire que l'on peut croire faible et sans ressources et qui, la plupart du temps, se présente comme le vengeur du peuple exploité ou dominé.

La cyberagression est en effet assimilée par ses auteurs à une riposte ingénieuse voire drôle, et en tout cas démocratique car elle émane d'une organisation qui se qualifiera de hackers patriotes, de défenseur des droits de l'homme, de cyberdissidents, de « foules intelligentes », de mouvement de démocratie directe, à une oppression dans le monde matériel ou immatériel. La punition, que nous évoquions plus haut est exaltée par la mise en scène d'une vengeance méritée du faible sur le fort.

Elle est renforcée par un effet « pilori » : les pays attaqués, les administrations ou les sociétés, voire les médias comme *l'Express* attaqué par Anonymous ou les journaux ciblés par l'AES

[158] Citation recopiée à l'article Anonymous de Wikipedia.

sont facilement conspués par un public qui est persuadé de prendre le parti du faible. Du retweet en témoignage d'indignation à la participation à une opération en ligne, ces internautes vont d'autant plus facilement s'engager. Au risque de partir sur de fausses pistes ou des canulars : fausse révélation que des parlementaires italiens vont consacrer des milliards d'euros du budget national à se recaser s'ils perdent leur mandat, fausse pétition contre la démolition d'une célèbre fontaine de Copenhague (que personne ne menaçait en réalité).

23 Dévoiler les secrets

231 Principe de révélation

Les technologies du Web ont également ouvert un vaste champ à une technique qui consiste à publier des documents authentiques et les rendre accessibles à des millions d'internautes en quelques secondes. Il est difficile de nier face à un texte, à un enregistrement, à des images prises dans les archives de la victime elle-même. Parlons, pour simplifier, de principe de la révélation. La quasi totalité des affaires livrées aux médias par Wikileaks ou par E. Snowden sont des révélations venues de l'intérieur, des courriels compromettants, des Power Point utilisés pour la formation des agents, bref des documents qui semblent authentiques. Un tel phénomène est à rapprocher du *whistelblowing*: les mémoires numériques encouragent les bureaucraties à stocker des millions de documents, en principe sécurisés et confidentiels, mais gérer de tels systèmes réclame des milliers d'employés. Parmi eux, la probabilité est forte qu'il s'en trouve un, comme Bradley Manning, qui éprouve des scrupules et vive mal l'opposition entre ses convictions et les secrets que dissimule l'organisation ; il « siffle » la faute en diffusant sa preuve auprès de sites spécialisées.

Les technologies numériques aident le lanceur d'alerte à reproduire et répandre les documents compromettants (Ellsberg, l'homme des papiers du Pentagone sous Nixon, avait eu à photocopier clandestinement 7000 pages pour les porter au *New York Times*). Il devient facile de devenir lanceur d'alerte à son tour : il suffit de profiter d'un micro mal coupé, d'une caméra qui continue à tourner ou simplement d'avoir un ordiphone sur soi quand un personnage public fait une gaffe.

Les technologies de diffusion, comme le découvrent les autorités turques au moment où nous écrivons ces lignes, font qu'une fois que l'information est « dans le tuyau », il est très difficile d'empêcher des millions d'internautes d'y avoir accès.

Dans ces conditions la technique de la révélation a de bonnes chances de jouer un rôle croissant dans les stratégies d'influence.

Il arrive que le document révélé soit faux ou retouché ou recontextualisé pour lui donner un sens scandaleux. Mais il arrive aussi que la source de la révélation affecte sa réception. Ainsi, la façon dont des propos d'une représentante américaine appelant « l'Europe à aller se faire foutre », une conversation entre responsables occidentaux examinant l'hypothèse que les tireurs de toits de Maïdan aient été des agents provocateurs et des déclarations de Mme Timochenko appelant au meurtre de Poutine et à l'usage de l'arme atomique contre les Russes ont été exploitées par la propagande du Kremlin a suscité aussitôt des contre-feux : la dénonciation des méthodes « héritées du KGB » dans la production de ces preuves que l'on déclarait truquées.

Révélations et trucages, métapropagande (accuser tout document favorable à l'adversaire d'être une fabrication de propagandistes professionnels[159]) semblent promis à un bel avenir à l'époque de l'enregistrement pirate et des sites relais.

24 Désinformation

C'est un nouveau champ pour la désinformation.

Le terme doit être défini avec rigueur pour ne pas se transformer en vague équivalent de « mensonge » (y compris le mensonge que l'on se fait souvent à soi-même par conviction idéologique). Par ailleurs, quelles que soient les critiques légitimes faites aux médias, à leurs biais, à leurs insuffisances, leurs stéréotypes, il faut réaffirmer que la déformation ou la mésinformation ne sont pas la désinformation.

Dans les années 1970/1980, ceux qui accusaient l'autre camp de désinformation étaient généralement anti-communistes ; ils se vantaient de dévoiler les fabrications des services soviétiques : source imaginaire du Sida, faux carnets d'Hitler, pseudo actions de la CIA.... toutes mises en scène dans un but idéologique : discréditer les Occidentaux. Ladite désinformation se pratiquait si possible en faisant parvenir à un média de réputation

[159] Voir la campagne en ligne lancée par des pro-israéliens contre le « Palywood » (une contractions de Palestiniens et Hollywood) et qui cherche à démontrer que la plupart des victimes civiles palestiniennes sont des comédiens qui font semblant d'être gravement blessés devant les caméras de la presse internationale.

internationale un faux document ou témoignage pour qu'il répande une accusation apparemment de source neutre.

Après la chute de l'URSS, à l'heure où le monde découvrait les chaînes d'information continue par satellite, la désinformation a changé de camp ou au moins d'usage : pseudo preuves et prétendues atrocités ont servi à justifier les guerres démocratiques ou humanitaires sur fond de *storytelling* et d'images bouleversantes.

Plus il y a de caméras numériques, de journalistes citoyens qui témoignent, de réseaux sociaux indignés contre les mensonges d'État, de vérificateurs des faits en ligne, plus la désinformation nous obsède... L'authenticité des « nouvelles » devrait être garantie par le nombre et la pluralité des sources. Or, la floraison des *tweets* et des images en direct n'apporte aucune certitude d'être moins dupe.

Le scepticisme de masse se répand (« la vérité est ailleurs », « tout est truqué ») et les explications alternatives prolifèrent, surtout sur la Toile. Quand un événement traumatise le public (comme le onze septembre), la controverse porte sur la vérité même des faits bruts qui ont pourtant eu des milliers de témoins. Par ailleurs les acteurs potentiels de la désinformation (à but économique, par exemple) prolifèrent et les amateurs peuvent s'y essayer avec des outils numériques simples.

Les entreprises, si soucieuses de leur e-réputation et d'une image citoyenne vivent dans la terreur de la crise de réputation, des rumeurs contagieuses, des mobilisations en ligne. Elles tendent à suspecter une désinformation délibérée menée par la concurrence, ce qui n'est pas toujours vrai.

243 Se méfier de la méfiance

Le citoyen de bonne foi - celui qui voudrait user de sa raison avec d'autres en se référant au même monde réel - doit se méfier des versions officielles acceptées avec une trop belle unanimité.

Mais il doit aussi se méfier de la méfiance et des contre-explications délirantes : celles qui nient les faits les plus avérés au nom de théories qui ne se soumettent pas à des procédures de vérification.

Au troisième degré, même l'accusation de « complotisme[160] » si souvent utilisée pour disqualifier les voix dissidentes doit être vérifiée : il faut démontrer la vérité ou la fausseté des faits, et ne pas se contenter de disqualifier, en utilisant des catégories idéologiques ou psychiatriques ceux qui s'y réfèrent.

Le tout se déroule sur fond de démocratisation des outils de désinformation : qu'il s'agisse de collecter des éléments pour une mise en scène, de modifier les contenus avec un logiciel de traitement de l'image, de s'anonymiser, de créer artificiellement des sources qui semblent concordantes, de mobiliser des communautés qui reprennent le message à leur compte, de tricher avec le référencement, de créer de faux partisans, etc[161]. C'est ce que démontrent de petits groupes qui semblent réaliser assez facilement des « exploits » comme celui de l'AES faisant baisser la bourse.

Et si, d'un côté, il existe de multiples procédés de *fact checking*, des équipes de professionnels qui critiquent la vraisemblance des images qu'ils reçoivent, des citoyens qui vont vérifier en ligne des affirmation d'hommes politiques ou des responsables économiques, la tendance inverse, celle qui favorise la « crédulité », n'est pas moins importante.

25 Le rôle multiplicateur des réseaux sociaux

Les réseaux sociaux sont d'excellents incubateurs de passions politiques, à commencer par l'indignation, mais aussi des sources d'interprétations concurrentes de la réalité.

Leur structure sociologique y aide : un système de conversation continue réunissant des acteurs qui ont des affinités et peuvent en principe participer de manière égale et anonyme. Pourtant, certains sont beaucoup plus égaux que d'autres. Certains facteurs sont favorables à l'esprit critique[162]. Profitant des facilités techniques, les plus experts ou les plus concernés dépensent parfois beaucoup d'énergie pour aider les autres à savoir la vérité.

---

[160] L'accusation de recourir à « l'éternelle théorie du complot » est devenue une figure de style récurrente des débats politiques.

[161] Voir Observatoire géostratégique de l'information, 16 janvier 2013 « Faux, rumeurs et désinformation dans le cyberespace » (http://www.iris-france.org/docs/kfm_docs/docs/observatoire-geo-info/2013-01-faux-rumeurs-et-desinformation-dans-le-cyberespace.pdf)

[162] Nous nous référons par là au fait que, sur Internet, des milliers de citoyens tentent de faire progresser la vérité, d'avertir de trucages ou mensonges qu'ils ont constatés ou d'aider les autres internautes à mieux se renseigner.

Les réseaux peuvent devenir des « bulles » qui protègent des informations contraires ou arguments dérangeants. Trois tendances jouent en ce sens :

- Le biais de confirmation - prédisposition à ne s'exposer qu'à des informations qui vont dans le sens souhaité et que fournissent surabondamment les autres contributeurs convaincus de la justesse de la cause ;

- l'isolement par rapport à l'opinion « moyenne », donc moins de chances de comprendre ce que pensent, pas forcément à tort, ses contemporains ;

- la dérive vers les positions les plus dures, en vertu du principe que ce sont souvent les plus extrémistes qui consacrent davantage d'énergie à prouver leurs thèses hors normes et à combattre la moindre objection[163].

Du point de vue des stratégies d'influence, les réseaux sociaux représentent donc des enjeux cruciaux, ne serait-ce que par leurs interactions avec les médias classiques et peuvent être des leviers puissants et déclencher des contagions imprévues comme ce fut le cas lors du printemps arabe. Même si la technologie peut donner un avantage relatif au tricheur (création de comptes de faux partisans crédibles, trucages) les stratégies d'influence et de contre-influence (subversion et contre-subversion si l'on préfère) doivent s'y inventer au quotidien.

Comme pour le discours persuasif, le jeu de l'influence, reproduit des schémas plus anciens, mais s'est incroyablement ouvert avec les technologies numériques. Le ticket d'entrée est à la portée de tous, et plus seulement des spécialistes, des administrations, des officines et des médias *mainstream*. Mais les conditions du succès (inventer un « mème[164] » qui soit repris, « *liké* », signalé, intériorisé par des millions de gens) sont plus complexes. Elles résultent de milliers de micro-décisions instantanées de gens qui cliquent, commentent, reproduisent et ainsi de suite. Et qui ont accès à de multiples sources.

[163] Voir la synthèse très claire de Gérald Bronner dans *La démocratie des crédules*, PUF, 2012

[164] Néologisme formé sur le modèle de « gènes » et qui désigne les unités de sens (images, terme, idée et ses déclinaisons) qui se reproduisent dans l'écosystème culturel, en particulier numérique.

Partie III - Recommandations pour la France

La prise de conscience de l'importance d'une cyberdéfense, voire d'une cyberstratégie, nécessaire pour notre pays, date de plus de dix ans si l'on prend pour point de départ le plan de renforcement des systèmes d'information de l'Etat décidé en 2004. Dès 2005, avec le rapport du député Pierre Labordes « La sécurité des systèmes d'information. Un enjeu majeur pour la France » est évoquée la défense des infrastructures vitales ou critiques du pays, qu'elles soient d'Etat ou privées.

Depuis le Livre blanc de 2008 qui décrit ces infrastructures comme des composantes cruciales de notre souveraineté et évoque notre capacité de lutte dans le cyberespace incluant la Lutte Informatique Offensive (LIO), il devient difficile de dire que la question a été négligée. Depuis, les initiatives se sont multipliées. Pour ne citer qu'une des dernières, le Pacte Défense Cyber de Défense présenté en février 2014 par le ministre de la Défense comporte cinquante mesures articulées autour de six axes (durcir le niveau de sécurité, intensifier l'effort de recherche, renforcer les ressources humaines dédiées, développer un pôle d'excellence cyber, cultiver un réseau de partenaires étrangers, favoriser l'émergence d'une communauté nationale de cyberdéfense). Si l'on ajoute les propositions portées par ce plan aux mesures préconisées par le rapport Bockel de 2012, aux objectifs stratégiques de l'ANSSI, aux directions indiquées par le Livre blanc de 2013 et à nombre de déclarations officielles ou textes de doctrine sur les voies et moyens de notre cyberdéfense, sur la posture à adopter en ces matières ou sur la résilience face à des attaques majeures, il faudrait de la mauvaise foi pour prétendre que les projets manquent.

Notre propos n'est pas de rajouter des propositions à celles qui existent. Il est moins encore de théoriser en chambre la réforme d'institutions dont certaines sont fort récentes, tant que l'avis des praticiens de terrain ne justifiera pas des changements drastiques.

Il nous semble plus utile de penser les grands axes d'une stratégie qui serait valable même si la défense de nos systèmes d'information se révélait techniquement imperméable et son organisation parfaitement coordonnée. Même si nos infrastructures étaient à l'abri du pillage de notre patrimoine informationnel - alors que la tendance globale semble être à l'augmentation numérique de ces attaques - et même si l'ensemble des mesures préconisées par les textes étaient appliquées à la satisfaction unanime, la nécessité d'une vision stratégique subsisterait.

Organisation

Quelques principes d'action et éléments de l'organisation de la cyberdéfense française pourraient être précisés:

- Les réseaux sociaux doivent être l'objet d'une veille spécifique, destinée à permettre des réactions immédiates. Ce sont des terrains d'analyse où se révèlent des tendances idéologiques et sociétales, mais aussi où il est possible de repérer les vecteurs des menaces (espionnage, sabotage, leurres, faux messages et faux mouvements d'opinion) qui demandent d'être prises en compte le plus tôt possible. Ces réseaux pourraient aussi diffuser des discours de justification de l'action de la France. Ils peuvent servir à attirer davantage d'attention ou à motiver plus d'alliés que le discours adverse, voire le contrer ou produire une certaine perturbation dans l'autre camp.

- Il faut mettre autant l'accent sur l'aspect humain et informationnel du cyberespace que sur les aspects techniques. Dans ce cadre, le Commandement des Opérations Spéciales (COS) dont l'expertise est reconnue dans le domaine de l'influence, notamment par le récent rapport du Sénat (525 ; 2013-2014) sur le renforcement des forces spéciales françaises, pourrait jouer un rôle de vecteur majeur. Le COS, par la spécificité de ses modes d'action, semble le cadre d'exécution logique d'une partie des opérations offensives dans le cyber, surtout liées à la couche sémantique comme les opérations psychologiques et d'influence. L'apport du cyber aux opérations d'influence peut se concevoir dans ce cadre avec l'appui des « 150 réservistes [du COS] tant ceux-ci occupent des fonctions utiles d'appui, de soutien voire de conduite dans certaines spécialités telles que la traduction, l'analyse ou les opérations d'influence » (p. 22).

- Toujours dans ce cadre, la question de la lutte subversive sur les réseaux sociaux doit être abordée de manière réaliste. Nos armées, lors de futures interventions extérieures, se trouvent confrontées à des groupes hostiles , terroristes, jihadistes ou autres, sur les réseaux sociaux. Par ailleurs, les prises de position de notre pays en matière de géopolitique l'amèneront sans doute à subir des attaques relevant de la désinformation ou de la subversion sur le Net. Nos forces armées, comme d'autres administrations exposées, sont, certes, présentes sur Facebook, Twitter, YouTube et autres réseaux sociaux, mais utilisent essentiellement ces médias pour présenter de l'information factuelle et répondre à des questions, comme celles de futures recrues. Il est impossible de faire l'impasse sur une dimension culturelle : beaucoup d'officiers répugnent à faire quelque chose qui ressemblerait aux opérations psychologiques menées au cours du XXe siècle, voire à pratiquer une communication qui dépasserait les limites de l'information purement factuelle, sans oublier la crainte de tenir un discours « politique ».Il ne s'agit pas d'imiter modèle américain, ni d'aller aussi loin que le modèle israélien, qui suppose un certain substrat idéologique unissant ses partisans en ligne. Mais il doit être possible de s'inspirer de réussites britanniques en

matière d'influence 2.0. Tout cela suppose à la fois des outils techniques et une organisation sachant réagir très vite, une coordination et sensibilisation des acteurs, mais aussi des argumentaires préparés à l'avance et des méthodes d'influence déjà pensées avant l'action.

- La coopération inter-agences de renseignement qui fonctionne déjà doit être poursuivie et améliorée avec une distribution plus claire des rôles entre DGSE, DGSI, DRM et DPSD.

- La question de la protection du patrimoine informationnel portée par les systèmes d'information des entreprises françaises implantées à l'étranger reste posée.

Crédibilité

Il s'agit de renforcer notre posture stratégique tous azimuts et de l'afficher très lisiblement.

Jusqu'à présent la présence effective de la France dans le cyberespace, contrairement à d'autres puissances comme les Etats-Unis, la Chine, la Russie ou Israël, a été discrète. Les déclarations officielles lorsque notre pays a fait l'objet soit d'intrusions ciblées contre l'Élysée, Bercy ou de grandes entreprises, soit d'une surveillance générale par le système de la NSA, dispositif dont on peut difficilement croire qu'il serve uniquement à repérer des jihadistes, témoignent de cette « stratégie du silence ».

Comme pour le nucléaire, une cyberstratégie doit être crédible pour être efficace. Le discours stratégique devient inséparable de l'arme d'autant qu'ici elle devient obsolète plus vite qu'une arme classique. Il ne suffit pas d'avoir la capacité technique, il faut aussi la démontrer et être crus.

Une puissance nucléaire doit avoir procédé à un essai ou une attaque pour être crédible mais pour autant devient-on une cyberpuissance une fois que l'on a procédé à une cyberagression de haut niveau ? Celle-ci démontre plusieurs choses : la performance technique, la qualité stratégique (espionnage préalable, identification de la cible, mise en place et déclenchement de la charge), enfin et surtout la détermination politique. L'arme n'est rien si elle n'est accompagnée - voire précédée - d'un discours approprié.

Or la France semble avoir choisi une politique de dédramatisation ou de protestation minimale lorsqu'elle est victime. Elle reste discrète sur ses armes offensives dont elle admet seulement l'existence.

Le premier point a un inconvénient immédiat : s'en tenir à des déclarations gênées, donner l'impression de tolérer beaucoup de choses surtout quand elles pourraient provenir d'alliés, donc admettre implicitement que tout le monde en fait plus ou moins autant et que chacun participe du même système. Dans le cas des révélations d'E. Snowden, la publicité donnée au système Frenchelon et à l'accord Lustre, quelle que soit la réalité qui se dissimule derrière, n'a pas aidé les autorités de notre pays à avoir une attitude aussi ferme que le Brésil ou l'Allemagne. Lors d'une prochaine échéance, il deviendrait nécessaire de prévoir un discours à la fois plus pédagogique et plus ferme. Il faut envisager une gamme de réponses diplomatiques ou économiques, en particulier dans les négociations internationales, sans entrer dans un processus d'escalade ; manifester sa contrariété n'implique pas de déclencher un conflit diplomatique ou économique.

Les armes offensives posent des problèmes différents. À titre provisoire, on peut se satisfaire de la position actuelle : laisser d'éventuels adversaires imaginer quelles armes offensives nous possédons sans leur en révéler la nature et à les convaincre de notre volonté de les utiliser s'il le faut. Ceci repose sur deux calculs : un agresseur ne prendra pas facilement le risque d'une rétorsion dont il ne peut mesurer la gravité ; il la craindra à la mesure de la résolution affichée par notre pays et de sa réputation d'excellence informatique.

Comment atteindre ce double objectif ? Il n'est pas seulement envisageable de procéder à des essais « à blanc » hors de toute situation stratégique et en laboratoire. Ceci n'empêche pas d'envisager des tests de simulation d'offensives contre nos défenses, voire contre nos grandes entreprises pour en tester la sécurité à la manière d'une sorte de *kriegspiel*, mais ceci est à usage interne.

Les gains sémantiques et stratégiques obtenus par les Etats-Unis à la suite de l'affaire Stuxnet, en termes de crédibilité de la volonté et des capacités, peuvent maintenant être appréciés. Ils pourraient inspirer une reflexion française.

Si nous devions un jour sortir l'arme mystérieuse du « placard », ce ne pourrait être que pour une action de sabotage, au sens des catégories exposées plus haut. On voit mal, en effet, un État démocratique pratiquer l'espionnage pour exercer une contrainte ou une rétorsion et l'avouer sur la place publique. Quant à une opération de subversion, notre culture, en particulier militaire, n'encourage guère à coopérer avec des hackers aux motivations idéologiques, par exemple. On imagine à quelles interprétations médiatiques prêteraient de telles opérations, dont, de surcroît, l'effet déstabilisateur ne serait pas immédiat.

Un dommage infligé à un adversaire par maliciel interposé se mesurerait en pertes financières ou en perturbation organisationnelle : retard des projets ou chaos gagnant ses systèmes d'information et de coordination. Se pose la question de la cible ; viser un Etat est hors de question, mais un important groupe terroriste ayant déjà agi contre la France pourrait constituer un objectif licite. Enfin, il faudrait que le dispositif soit suffisamment remarquable par sa qualité technologique ou son innovation, pour être relevé par la presse internationale. Mais si un jour nous devions mener une action similaire à Stuxnet ou à Gauss (contre le financement d'un groupe terroriste), nous ne pourrions pas le reconnaitre officiellement mais devrions demeurer dans le registre du faire-savoir.

> *Une stratégie de communication ne revendiquant rien officiellement mais faisant comprendre que la France ne désapprouve pas, crédibiliserait la posture adoptée.*
>
> *Encore faut-il que l'adversaire fournisse l'occasion et la justification et que la France soit prête à pratiquer cette forme particulière de rétorsion/démonstration. Pour cela il faudrait sans doute constituer l'équivalent plus offensif d'une cellule de crise. Elle préparerait des scénarios, envisagerait les conséquences y compris économiques, intègrerait la dimension sémantique, voire médiatique, à l'action. Le facteur temps étant crucial, il importe qu'une procédure rapide de décision et de feux verts soit mise en place, et que les débats soient menés et les choix opérés en amont.*
>
> *Il s'agirait de passer d'une attitude de simple réaction à une posture plus proactive. Elle présuppose un renseignement fiable, humain et pas seulement technologique, qui aide les décideurs à savoir à la fois qui est susceptible de nous attaquer dans le cyber, comment et dans quel but, quelles sont ses vulnérabilités et d'imaginer ses réactions s'il était frappé à son tour.*

Position internationale

Le système de la NSA décrit par Snowden est d'une telle démesure que cela constitue un « cliquet d'irréversibilité ». Un tel dispositif servant à prélever des données et métadonnées et à les corréler pour anticiper des comportements n'a plus rien à voir avec une époque où l'espionnage était une activité ciblée et plus ou moins tolérée entre puissances. Il va au-delà d'une problématique de libertés publiques. Il s'agit d'un changement de statut : espionnage, surveillance, contrôle et anticipation fusionnent en un projet de total « information awareness » portant sur des milliards de données et instaurent un nouveau rapport de forces dans le cyberespace.

Les effets ont été considérables sur les grandes compagnies du Net placées dans la situation embarrassante de complices et victimes à la fois, sur le système de gouvernance d'Internet (ce

dont témoignent des velléités de réforme de l'ICANN), sur l'opinion publique internationale, sur la création de solutions alternatives sécurisées et, accessoirement, sur quelques gouvernements (Brésil, Argentine, Allemagne) qui sont allés au-delà des protestations embarrassées. Enfin, des pays comme la Chine ou la Russie ont vu leurs discours sur la régulation du cyberespace crédibilisé.

C'est pour notre pays l'occasion de réaliser que la cyberstratégie doit s'intégrer dans une vision géopolitique, voire géoéconomique, et ne pas seulement être pensée en termes de sécurité. La position internationale de notre pays sur la gouvernance d'Internet, ses choix de solidarité avec ses alliés en matière de cybersécurité et ses positions face à la balkanisation du Net ne peuvent désormais plus se séparer du souci sécuritaire initial.

> *Il reste donc à trouver une position plus lisible entre des challengers de l'ordre actuel qui veulent plus de contrôle et moins de libertés publiques (Chine, Russie) et les tenants de ce même ordre (Etats-Unis) qui tirent profit de leur domination du système.*
>
> *Une posture plus indépendante et souveraine rencontrerait la faveur du public, sans dégrader l'image de la France. Sans rejoindre un camp pro-russe ou pro-chinois, cette posture contrasterait avec l'ambiguïté actuelle. Elle renforcerait une politique qui se veut de soft power ou d'influential power et pourrait rallier de nombreux pays sur des questions de régulation.*
>
> *En se rapprochant peut-être de la position brésilienne - contester la domination américaine au niveau global, sans tomber dans la censure et le contrôle au niveau national - la France pourrait prendre la tête d'un groupe de pays aux positions se situant entre celles des Etats-Unis et celles de la Chine ou de la Russie.*
>
> *Lors de la dernière réunion de Rio, qui, il est vrai, n'a pas débouché sur une grande évolution, la position de la France n'a pas été très lisible. Elle est peut-être diplomatiquement nuancée mais se réduit, pour le grand public, à un alignement sur les positions américaines.*

Les normes

Pour compléter cette posture, il est utile de conduire quelques autres actions adaptées au nouvel environnement du cyberespace, à la fois plus international et global et de mettre l'accent sur les normes techniques, juridiques ou culturelles.

> *La France devrait développer son influence normative dans les instances internationales. Si les Français sont présents dans certaines comme l'ISA, l'idée est de développer d'un côté une véritable stratégie coordonnée public-privé et de l'autre de nouer des alliances avec nos partenaires européens pour avoir plus de poids dans les débats. Le volet de normalisation technologique entrepreneurial est prioritaire. Il faudrait dans ce cadre créer une alliance/partenariat entre acteurs européens de l'IT*

pour aboutir à des normes continentales.

La francophonie est un forum insuffisamment utilisé. Si l'on suit les prévisions de croissance de la présence africaine sur Internet, le français, langue minoritaire pour le moment, devrait d'ici quelques décennies devenir une des langues majeures du cyberespace. Il serait utile pour la France de profiter de ce développement du français dans un cadre de balkanisation du Net pour échapper partiellement au modèle anglo-saxon.

Index

Bibliographie

Ouvrages

ACHARD P. et BERNAT J-P., *L'intelligence économique : mode d'emploi*, ADBS Editions, 1998.
ALMEIDA F., *Images et propagande*, Castermann, 1995.
ANDERSON, R.H. and HEARN, A.C., *An exploration of cyberspace Security R & D Investment Strategies for DARPA*, Rand Corporation, 1997.
ANDREW, N. YANG, D. and LIAO, W.C., *PLA Rapid reaction forces: concept, training and preliminary Assessment* in J.C Mulvenon and R.Yang (eds), *The People's Liberation Army in the Information Age*, Rand Corporation, 1999.
ARENDT H., *Mensonge et politique* in *La crise de la culture*, Gallimard, 1963.
ARENDT H.., *Du mensonge à la violence*, Calmann-Lévy, 1972.
ARISTOTE, *Rhétorique*, Les Belles Lettres.
ARPAGIAN N., *La Cyberguerre – La guerre numérique a commencé*, Vuibert, 2009.
ARPAGIAN N., *La Cybersécurité*, Presses Universitaires de France, 2010.
ARQUILLA J. et RONFELDT D., *The emergence of noopolitik : toward an American Information Strategy*, Rand Corporation, 1999.
ARQUILLA J. et RONFELDT D., *Networks and Netwar : the Future of Terror, Crime and Militancy*, Rand, 2002.
ARQUILLA J. et RONFLEDT D., (sous la direction de), *In Athena's camp : Preparing for Conflict in the Information Age*, Rand Monograph Report, Rand, 1997.
ASSANGE J., *Menace sur nos libertés*, Robert Laffont, 2013
AUGÉ E., *Petit traité de propagande à l'attention de ceux qui la subissent*, Ed. De Boeck Université, 2007.
BAILLARGEON N., *Petit cours d'auto-défense intellectuelle*, Lux 2007.
BARBER B., *Jihad vs McWorld*, New York, Random House, 1995.
BATESON et al., *La nouvelle communication*, Seuil, 1984.
BAUDRILLARD J., *La guerre du Golfe n'a pas eu lieu*, Galilée, 1991.
BAUER, A. et HUYGHE, F.B., *Les terroristes disent toujours ce qu'ils vont faire*, PUF, 2008.
BAUTIER R., *De la rhétorique à la communication*, PUG 1994.
BEAUDOUIN JP, *Etre à l'écoute du risque d'opinion*, Editions d'organisation, 2001.
BEAUFRE A., *Introduction à la stratégie*, Hachette Pluriel 2009.
BEAUVOIS J.L. et JOULE R.V., *La soumission librement consentie – Comment amener les gens à faire librement ce qu'ils doivent faire ?*, PUF, 1998.
BEAUVOIS J.L. et JOULE R.V., *Petit traité de manipulation à l'usage des honnêtes gens*, PUG 1987.
BECK U, *Pouvoirs et contre-pouvoirs à l'heure de la mondialisation*, Editions Aubier, 2003.
BENASSAYAG M., Sztulwark D., *Du contre-pouvoir*, La Découverte, 2002.
BENKLER, Y., *The wealths of networks*, Yale University Press, 2004.
BERKOWITZ B., *The Next Face of War*, The Free Press 2003.
BERNAYS E., *Propaganda, comment manipuler l'opinion publique en démocratie*, Zones,

2007.
BERGER J.M. & STRATHEARN B.,*Who Matters Online : Measuring influence,evaluating content and countering violent extremism in online social networks*, Lomdres, The International Centre for the Study of Radicalisation and political violence, 2013
BERTHO-LAVENIR C., *La démocratie et les médias au XXe siècle*, A. Colin, 2000.
BESON B. et POSSIN J.C., *Du renseignement à l'intelligence économique*, Dunod, 1996.
BEY H, T.A.Z., *Zone autonome temporaire*, L'éclat 1998.
BLOCH A., *L'intelligence économique*, Economica, 1996.
BOCKEL J.-M., *Rapport d'information sur la cyberdéfense*, Sénat, juillet 2012
BOLER, M. (ed.), *Digital Media and democracy : tactics in hard times*, MIT Press, 2008.
BOORSTIN D., *L'image*, 10-18, 1967.
BOUDON D., *L'art de ses persuader des idées douteuses, fragiles ou fausses*, Seuil, Points, 1990.
BOUGNOUX D., *La communication contre l'information*, Hachette, Questions de Société, 1995.
BOUGNOUX D., *Introduction aux sciences de la communication*, La Découverte, 2002.
BOURDIEU P., *Ce que parler veut dire - L'économie des échanges linguistiques*, Fayard, 1982.
BOUTHOUL G., *Traité de polémologie*, Payot, 1962.
BOYER B., *Cyberstratégie, l'art de la guerre numérique*, Nuvis, 2012.
BRETON P., *Le culte d'Internet*, La Découverte, 2000.
BRETON P., *Convaincre sans manipuler*, La Découverte 2008.
BRETON P., *La parole manipulée*, La Découverte, 1997.
BRONK C. et TIKK-RINGAS E., *Hack or Attack ? Shamoon and the Evolution of Cyber Conflict*, James A Baker III Institute for Public Policy – Rice University Working Paper, février 2013.
BRONNER, G., *La démocratie des crédules*, Paris, PUF, 2012.
BRZEZINSKI Z., *La révolution technétronique*, Calmann-Lévy, 1971.
CAMPBELL D., *Surveillance électronique planétaire*, Allia. 2001.
CAMPEN A.D., *The first Information War : The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War*, Fairfax : AFCEA, 1992.
CARDON D., *La démocratie Internet : promesses et limites*, Seuil 2010.
CARR J., *Inside cyberwarfare*, O'Reilly Media; 2009.
CASILLI A., *Les liaisons numériques, vers une nouvelle socialité*, Seuil 2010.
CASTELLS, M., *L'ère de l'information*, 3 tomes, Fayard, 1998, 1999, 1999.
CASTELLS, M., *The Internet galaxy : reflections on the Internet, Business and Society*, Oxford University Press, 2001.
CHAIX N. (dir.), *Economie et sécurité : de l'industrie de défense à l'intelligence économique*, FED, Coll. Perspectives Stratégiques, 1996.
CHALIAND G., *Les guerres irrégulières XXème- XXIème siècle*, Gallimard, 2008.
CHALIAND G., *Anthologie mondiale de la stratégie*, R. Laffont 1996.
CHARLOT M., *La Persuasion politique*, Armand Colin, 1970.
CHARON J. M.et MERCIER A. (dir.), *Armes de communication massive - Information de guerre en Irak 1991-2003*, CNRS, 2004.
CHATHAM HOUSE, *Cybersecurity and International Law*, Meeting Summary, mai 2012.
CHATHAM HOUSE, *Beyond Borders: Digital Activism in a Glogalized World*, Meeting

Transcript, février 2012.
CLARKE R. et KNAKE R., *Cyberwar : the Next Threat to National Security and What to do About It*, Ecco Press 2010.
CHOMSKY N. et HERMAN E, *La fabrication du consentement: de la propagande médiatique en démocratie*, Agone, 2008.
CHOMSKY N., *Propagande, médias, démocratie, avec Robert W. McChesney*, Ecosociété, 2000.
COLLECTIF (Kim CRAGIN, Peter SCHALK, Sara A.DALY et Brian A.JACKSON), *Sharing the Dragon's Teeth – Terrorist Groups and the Exchange of New Technologies*, Rand, 2007.
COLLECTIF, *Livre Blanc sur la Défense et la Sécurité Nationale*, Editions Odile Jacob-La Documentation Française, juin 2008.
COLLECTIF, *A cCollection of Papers of the International Symposium on Cyber Security : China and the World,* May 28-29, Beijing, CHina
CORNISH P., *The Vulnerabilities of Developed States to Economic Cyber Warfare*, Chatham House, 2011.
CORNU D., *Ethique de l'information*, PUF, 1997.
COTTLE, S., *Mediatized Conflict : developments in media and conflict studies*, Open University Press, 2006.
COUTAU-BÉGARIE O., *Traité de stratégie*, Economica, 2011.
CSIS (The Center for Strategic and International Studies), *Securing Cyberspace for the 44th President*, Report of the CSIS Commission on Cybersecurity for the 44th Presidency, 8 décembre 2008.
DAGNAUD M., *Le web ce laboratoire du capitalisme sympa,* in Le débat, 2010-3, pp. 161-176.
DELESSE, C., *Echelon et le renseignement électronique américain*, Editions Ouest-France, 2012.
CREEL G., *How we advertised America*, Harper & Brothers, 1920.
D'AVENI R., *Hypercompetition*, Free Press, 1994.
DAHMANI A. (dir.), *La démocratie à l'épreuve de la société numérique*, Gemdev Karthala, 2007.
DARTNELL M., *Insurgency Online : Web Activism and Global Conflict*, University of Toronto Press, 2006.
DEBORD G., *La société du spectacle*, Buchet Chastel, 1967.
DEBRAY R., *Cours de médiologie générale*, Gallimard, 2001.
DEBRAY R., *L'État séducteur*, Gallimard, 1993.
DELBECQUE E., *L'intelligence économique*, PUF, 2006.
DELER J.P., Fauré Y.-A., Piveteau A. et Roca P.J., *ONG et développement*, éd. Karthala, 1998
DEMCHAK C., *Wars of Disruption and Resilience : Cybered Conflict*, Power and National Security UGA Press 2011.
DERVILLE G., *Le pouvoir des médias*, PUG, 1997.
DOBSON, W.G., *The Dictator's Learning Curve*, New York, Anchor Books, 2012.
DOMENACH J.M. *La Propagande politique*, PUF, 1969.
DOSSÉ S. et KEMPF O., *Stratégies dans le cyberespace*, éd. L'esprit du livre, 2011.
DOSSÉ S., KEMPF O. & MALIS C., *Cyberespace, nouveau domaine de la pensée stratégique*, Economica, 2013.

DUCATTE J.C., *La Gestion de l'influence*, Liaisons, 1998.
DUNNIGAN, J.F., *The next war zone: confronting the global threat of cyberterrorism*, Osborne-McGraw-Hill, 2002.
DURANDIN G., *L'information, la désinformation et la réalité*, PUF, 1993.
ECO, U., La guerre du faux, Gallimard, 1967, Grasset, 1985.
ELLUL J., *Histoire de la propagande*, PUF, 1967.
ELLUL J., *Propagandes*, A Colin, 1962, Economica, 1990.
ETTIGHOFER D., *L'entreprise virtuelle*, Odile Jacob 1992.
EWEN S., *Consciences sous influence*, Aubier, 1993
FAYARD P., *Comprendre et appliquer Sun Tzu*, Dunod, 2004.
FAYARD P., *Le réveil du samouraï Culture et stratégie japonaise dans la société de la connaissance*, Dunod, 2006.
FAYARD P., *La maîtrise de l'interaction*, Éditions 00H00, 2000.
FAYON D., *Géopolitique d'Internet Qui gouverne le monde ?,* Economica*, 2013*
Fondation pour les études de défense, *Les manipulations de l'image et du son*, Hachette, 1996.
FOGEL J.F. et PATINO B., *La condition numérique*, Grasset, 2013
FONTAINE R. et ROGERS W., *Internet Freedom: A Foreign Policy Imperative in the Digital Age*, Center for a New American Security, 2011.
FOUCAULT, *Surveiller et punir*, Gallimard 1975.
FRANCART L., *La guerre du sens*, Economica, 2000.
FRANCART L., *Infosphère et intelligence stratégique*, IHEDN-Economica, 2002.
FRANCOIS L. (sous la direction), *Business sous influence*, Editions d'Organisation, 2004.
FREEMAN R.E., PIERCE J., DODD H., *Environmentalism and the New Logic of Business*, éd. Pitman. 2002.
FREEMAN R.E., *Strategic management : a stakeholder approach*, Pitman, 1984.
FRESNAULT-DESRUELLES, *L'image manipulée*, Edilig, 1983.
FREUD S., *Psychologie collective et analyse du Moi*, Payot 1950.
FREUND A., *Journalisme et mésinformation*, Grenoble, La Pensée Sauvage, 1991.
FRIEDMAN M., *Capitalisme et Liberté*, Robert Laffont, 1971.
GANLEY O. H. and Ganley, G. D., *To inform or to control? The new communication networks*, NY: Ablex Publisher, 1989.
GÉRÉ F., *La guerre psychologique*, Economica, ISC1997.
GERVEREAU L., (sous la direction de), *Dictionnaire mondial des images*, Nouveau Monde, 2006.
GERVEREAU L., *Les images qui mentent. Histoire du visuel au XX siècle*, Seuil, 2000.
GIULIANI J.-D., *Marchands d'influence*, Seuil, 1991.
GOUREVITCH C., *La propagande dans tous ses états*, Flammarion, 1981.
GRANET D. et LAMOUR C., *Médiabusiness le nouvel eldorado*, Fayard 2006.
GRANJON F, *L'Internet Militant*, Editions Apogée, 2001.
GRANT R., *Victory in Cyberspace*, Air Force Association des Etats-Unis, 2007.
GRAY C., *La guerre au XXIe siècle*, Economica 2007.
GREENWALD, G., *Nulle part où se cacher*, J.-C. Lattès, 2014.
GRITTI, J., *Feu sur les médias*, Centurion, 1992.
GRUSELLE B., TERTRAIS B. et ESTERLE A., *Cyberdissuasion*, FRS, mars 2012.
GRUSINSKI S., *La guerre des images*, Fayard, 1990.

GUICHARDAZ P., LOINTIER P., ROSE P., *L'infoguerre*, Dunod, 1999.
GUIDÈRE M., *Histoire immédiate du printemps arabe*, Le Débat, 2012-1.
GUILLAUME M., *L'empire des réseaux*, Descartes et Cie, 2000.
GUISNEL J., *Guerre dans le cyberspace*, La Découverte, 1995.
HALIMI S. et VIDAL D., *L'opinion, ça se travaille. Les médias et les guerres justes*, Agone 2004.
HANSON, V., *Le modèle occidental de la guerre. : La bataille d'infanterie dans la Grèce classique*, Belles lettres, 1990, édition consultée : Tallandier Texto, 2007.
HARBULOT C., *Techniques offensives et guerre économique*, La Bourdonnaye, 2012.
HARBULOT C., (dir), *Manuel d'intelligence économique*, PUF, 2012 (1e ed et 2014 2e ed).
HARBULOT C., et LUCAS D. (dir.), *La guerre cognitive – L'arme de la connaissance*, Lavauzelle, 2002.
HARTMANN, F., *Lanceurs d'alerte : les mauvaises consciences de nos démocraties*, Ed. Don Quichotte, 2014.
HAZAN E., *LQR la propagande au quotidien*, Raison d'agir, 2006.
HECKER M. et RID T., *War 2.0: Irregular warfare in the information Age*, Praeger, 2009.
HEUSER, B., *Penser la stratégie de l'Antiquité à nos jours*, Editions Picard, 2013.HOFFMAN, B., *The use of Internet by Islamic Extremists*, Permanent Select Committee on Intelligence, 2006.
HOLLOWAY J., *Change the world without taking power*, Pluto Press, 2002.
HUYGHE F.B., *Écran/Ennemi Terrorismes et guerres de l'information*, éditions OOhOO, 2001.
HUYGHE F-B, *Maîtres du faire-croire, De la propagande à l'influence*, Vuibert, 2008.
HUYGHE, F.B., *L'ennemi à l'ère numérique*, PUF, 2001.
IPA, *The Fine Art Of Propaganda; A Study of Father Coughlin's Speeches*, by The Institute for Propaganda Analysis, Harcourt, Brace and Company,1939.
JABBAR J. AUDAH Al-Obaidi and WILIAM G., Jr., *Broadcast, Internet, and TV Media in the Arab World and Small Nations: Studies in Recent Developments*, Edwin Mellen, 2010.
JAKOBIAK F., *L'intelligence économique en pratique*, Les Editions d'Organisation, 1998.
JIAN M., *China's Internet Dictatorship*, Project Syndicate, 2005.
JORDAN T., *S'engager les nouveaux militants, activistes, agitateurs*, Collection Frontières, Autrement, 2003.
JORDAN, T., *Activism ! Direct Action, Hacktivism and the future of society*, Reaktion Books, 2002.
JORION, P., *La guerre civile numérique*, Textuel 2011.
JOWETT G.S. et O'Donnell V., *Propaganda and Persuasion*, CA: SAGE Publications, 1999.
JULLIARD J., *La reine du monde*, Flammarion 2008.
JULLIEN, F., *La propension des choses*, Seuil, 1992.
KAGAN R., *Le revers de la puissance*, Plon 2004.
KAGAN R., *La puissance et la faiblesse,* Plon 2002.
KAHANER L., *Competitive intelligence*, Simons & Shuster, 1996.
KAPFERER J.N., *Les chemins de la persuasion,* Gaultier-Villars, 1978.
KAUFFER R., *L'arme de la désinformation*, Grasset, 1999.
KEMPF O., *Introduction à la cyberstratégie*, Economica, 2012.
KEMPF, O.(dir), *Penser les réseaux*, L'Harmattan, 2014.
KLEIN N., *No Logo La tyrannie des marques*, Lémeac/Actes Sud, 2001.
KOJEVE A., *La notion d'autorité*, Gallimard 2004.

LAIDI A. et LANVAUX D., *Les secrets de la guerre économique,* Seuil, 2004.
LÉVY P., *Qu'est-ce que le virtuel ?*, La Découverte, 1995.
LÉVY P., *Cyberdémocratie : essai de philosophie politique*, Odile Jacob, 2007.
LIANG Quiao & XIANGSUI Wang, *La Guerre hors limites*, édition originale 1999. Traduction française, Editions Payot & Rivages, 2003.
LIBICKI M., *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge University Press, 2007.
LIBICKI M.C., *What is Information Warfare ?*, Washington, National Defence University, Institute for National Strategy Studies, 1996.
LIBICKI M., *Cyberdeterrence and Cyberwar*, RAND, 2009.
LINEBARGER P., *Psychological warfare*, New York, Arno Press, 1972.
LUCAS D. et TIFFREAU A., *Guerre économique et information*, Ellipses, 2001.
LUTZ W., *Doublespeak Harper Perennial*, 1990.
MAISONNEUVE E. de la, *Stratégie Crise et Chaos*, Economica, 2005.
MARCON C. et MOINET N., *La stratégie réseau*, Éditions OOHOO, 2003.
MARTIN D. et F.-P., *Cybercrime : menaces, vulnérabilités et ripostes*, P.U.F., 2001.
MASSÉ G. et THIBAUT F., *Intelligence économique : un guide pour une économie de l'intelligence*, Editions de Boeck, 2000.
MATTELART A., *Histoire de la société de l'information*, La Découverte, 2001.
MATTELART A., *L'invention de la communication*, La Découverte,1994 et 1999.
MATTELART A., *Histoire des théories de la communication*, La Découverte,1995.
MATTELART A., *La globalisation de la surveillance – Aux origines de l'ordre sécuritaire*, Editions La Découverte, 2007.
MARTEL F., *Mainstream*, Flammarion, 2011.
MARTEL F., *Smart*, Flammarion 2014
Mc LUHAN M. et FIORE Q., *Guerre et paix dans le village planétaire*, R. Laffont, 1970.
MC LUHAN M., *Pour comprendre les media*, Mame, 1968.
Mc LUHAN M., *The Medium is the Massage: An Inventory of Effects*, Books Bantam, 1967.
MERCER D., *The Fog of War*, Londres, Heinemann, 1987.
MILLER C., *Propaganda Analysis*, NY: Institute for Propaganda Analysis, 1937.
MONDAGE J., *Une industrie nouvelle : la fabrication de l'opinion publique*, Hirondelle, 1950.
MONDZAIN M.J., *Une image peut-elle tuer ?*, Bayard, 2005.
MORELLI A., *Principes élémentaires de propagande de guerre*, Labor, 2001.
MORIN E., *L'esprit du temps*, Grasset, 1976.
MOROZOV E., *The Net dellusion*, Public Affairs Books, 2011.
MOROZOV, E., *To Save Everything, Click Here: The Folly of Technological Solutionism*, Philadelphie, Public Affairs, 2014.
MOSCOVICI S., *L'Âge des foules*, Complexe, 1985.
MUCHIELLI A., *L'art d'influencer,* A. Colin, 2000.
MUHLMANN G., *Du journalisme en démocratie*, Petite Bibliothèque Payot, 2006.
MURAWIEC L., *La guerre au XXIe siècle*., Odile Jacob, 2000.
MYARD J., *La France dans la guerre de l'information*, L'Harmattan, 2006.
NEGRI T. et Hardt M., *Multitude*, La Découverte, 2004.
NOCETTI J., *La diplomatie d'Obama à l'épreuve du web 2.0*, in Politique étrangère,

2011-1.
NYE J., *Bound to lead*, Basics Books, 1991.
NYE J., *The Paradox of American Power*, Oxford University Press, 2002.
NYE J.S., *Cyberpower*, Harvard University, 2010.
NYE J., *Power and National Security in Cyberspace*, in LORD K. et SHARP T. (dir.), *America's Cyber Future vol. II*, Washington, Center for a New American Security, Juin 2011.
OCDE - *Comité de la politique de l'Information, de l'Informatique et des Communications. Groupe de travail sur la sécurité de l'information et la vie privée*, réf. DSTI/ICCP/REG (2007) 20/FINAL, 8 avril 2008.
PACKARD V., *La Persuasion clandestine*, Calmann-Lévy, 1958.
PERLAS N., *La société civile troisième pouvoir*, Ed Yves Michel, 2003.
PISANI F. et PIOTET D., *Comment le web change le monde: des internautes aux webacteurs*, Pearson, 2011.
PONSONBY A., *Falshood in Wartime* (1928), Republié par the Institute of Historical Review,
1991.
PUISEUX H., *Les figures de la guerre*, Gallimard, 1997.
QUENTIN P., *La propagande politique*, Plon, 1943.
STEINER G., *Les logocrates*, L'Herne 2003.
RAMONET I., *L'explosion du journalisme, des médias de masses à la masse des médias*, Galilée, 2011.
RAMONET I., *Propagandes silencieuses*, Galilée, 2000.
RAMONET I., *La tyrannie de la communication*, Galilée, 1999.
RAMPTON S. and STAUBER, J., *Trust Us, We're Experts: How Industry Manipulates Science*
and Gambles With Your Future, Tarcher/Putnam, 2001.
RAMPTON S. et STAUBER J., *L'industrie du mensonge - Lobbying, communication, publicité & médias*, Agone, 2004.
RAMPTON S. et STAUBER J., *Une arme de persuasion massive - De la propagande dans la guerre de Bush en Irak*, Le Pré aux clercs, 2004.
RAYNAUD P., *L'Art de manipuler*, Ulrich, 1996.
REBOUL A. et MOESCHLER J., *La pragmatique aujourd'hui*, Seuil, 1998.
REBOUL O., *Langage et idéologie*, PUF, 1980.
RENAUT A., *La fin de l'autorité*, Flammarion, 2006.
Rencontres Internationales Média-défense 1995 - Imagina, *Les manipulations de l'image et du son*, Pluriel, Hachette, 1996.
REVELLI C., *Intelligence stratégique sur Internet*, Dunod, 1998.
RHEINGOLD H., *Foules intelligentes. La révolution qui commence*. M2 éditions, 2005.
RINNAWI K., *The Internet and the Arab world as a virtual public sphere, Internet, Ben Gurion,* University of the Negev, 2012.
RID T., *Cyber War Will Not Take Place*, Oxford University Press, 2013
RIFKIN J., *L'âge de l'accès*, La Découverte, 2000.
ROBIN A., *La fausse parole*, Le Temps qu'il fait, 2002.
ROBINSON S., *The CNN effect : the myths of news, foreign policy and intervention*, Routledge, 2002.
RODRIK D., *The globalization paradox*, Norton, 2011.
ROETTER C., *Psychological warfare,* Bastford, 1974.

ROMANI R., *Rapport d'information n°449 sur la cyberdéfense*, Commission des Affaires étrangères, de la défense et des forces armées, Sénat, 8 juillet 2008.
ROSANVALLON P., *La contre-émocratie,* Seuil, 2006.
SALMON C., *Storytelling*, Editions La Découverte , 2007.
SANGER, D., *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, NYC, Crown, 2012.
SCHECHTER, D., *Media wars: news at a time of terror*, Rowman & Littlefield, 2003.
SENETT R., *Les tyrannies de l'intimité*, Seuil, 1990.
SFEZ L., *Critique de la communication*, Seuil, 1988.
SHIRKY C., *Cognitive Surplus, Creativity and Generosity in a Connected Age*, Penguin, 2010.
SHIRKY, C., *Here Comes Everybody: The Power of Organizing Without Organizations*, Londres, Penguin, 2008.
SIMPSON C., *Science of Coercion: Communication Research and Psychological Warfare, 1945-1960*, Oxford University Press, 1994
SLOTERDJIK, P., *Colère et temps*, éditions Maren Sell, 2007.
STIENNON R., *Surviving Cyberwar*, Government Insitutes, 2012.
STIGLITZ J., *La grande désillusion*, Paris, Plon, 2003.
STONOR SAUNDERS F, *Qui mène la danse ? La CIA et la Guerre Froide culturelle*, Denoël, 2003.
STORA B., *Imaginaires de Guerre*, La Découverte, 1997.
STUART E., *PR! A Social History of Spin*, New York, Harper Collins, 1996.
STUART E., *Consciences sous influences*, Editions Aubier Montaigne, 1983.
TALEB N., *Le cygne noir*, Les belles lettres, 2010.
TCHAKHOTINE S., *Le Viol des foules par la propagande politique*, Gallimard, 1952.
TOFFLER A et H, *Les Nouveaux pouvoirs*, Fayard, 1999.
TOFFLER A. & H., *Guerre et contre-guerre*, Fayard, 1994.
US Department of Defense, *Defense Science Board, Resilient Military Systems and the Advanced Cyber Threat*, Washington, USDoD, 2012.
VENTRE D. (dir), *Cyberguerre et guerre de l'information*, Lavoisier, 2010.
VENTRE D., *Cyberattaque et cyberdéfense*, Lavoisier, 2011.
VENTRE D., *Cyberespace et acteurs du conflit*, Lavoisier, 2011
VENTRE D., *La guerre de l'information*, Paris, Lavoisier, 2007.
VICTOROFF D., *La publicité et l'image*, Denoël/Gonthier (Médiations), 1978.
VIDINO, L., *Al-Qaeda in Europe: the new battleground of international Jihad*, Prometheus, 2006.
VIRILIO P., *La bombe informatique*, Galilée 1998.
VIRILIO P., *Stratégie de la déception*, Galilée, 1999.
VOLKOFF V., *Petite histoire de la désinformation*, Editions du Rocher, 1998.
VOLLE M., *Géopolitique du cyberspace*, in P. HASSNER, *Les Relations internationales*, Documentation Française, 2012.
WATZLAWICK P. (dirigé par), *L'invention de la réalité. Comment croyons-nous ce que nous croyons savoir ?,* Seuil, 1992.
WATZLAWICK P., *La réalité de la réalité - Confusion, désinformation, communication*, Seuil, 1978.
WAUTELET, M., *Les Cyberconflits*, GRIP / Complexe, 1998.

WEIMANN, G., *Terror on the Internet: the new arena, the new challenges*, United States Institute of Peace Press, 2006.
WOLTON D., *Penser la communication*, Flammarion, 1998.
WOLTON D., *Internet et après ?,* Flammarion, 2003.

Articles et revues

AGIR (F.B. Huyghe dir), *Puissance et influence n°14*, E. de la Maisonneuve, 2003.
AGUIOTIN C. et CARDON D., « The Strength of Weak Cooperation : An attempt to Understand the Meaning of Web2.0 », *Communications & Strategies*, n°65, 1st quarter, 2007.
AILLERET C., « Défense "dirigée" ou défense "tous azimuts" », *Revue de défense nationale*, décembre 1967.
AMBINDER M., « The Revolution will be Twittered », *The Atlantic*, 15 Sept 2009.
ANSSI, Défense et SSI, *Stratégie de la France*, 15 février 2011.
ARQUILLA J. et RONFELDT D., « Cyberwar is coming ! » in *Comparative Strategy*. Vol.12, N°2, Printemps 1993.
BEST M.L. et WADE K.W., « The Internet and Democracy, Global Catalyst or Democratic Dud ? », *Bulletin of Science, Technology and Society*, 2009.
BETZ D., « Cyberpower in strategic affairs: neither unthinkable nor blessed », *Journal of strategic studies*, nov. 2012.
BWELE C., « Peut-on dissuader dans le cyberespace ? », *Revue Défense Nationale*, Juin 2010.
CAHIERS DE MÉDIOLOGIE (revue), *Pourquoi des médiologues ?*, N° 6, 1998 et Communiquer /transmettre n° 11, Gallimard, 2001.
CAHIERS DE MÉDIOLOGIE, *Les cahiers de médiologie, une anthologie* (articles publiés 1996 et 2004), CNRS Éditions, 2011.
CHAUVANCY F., *La stratégie d'influence par la maîtrise de l'information*, dossier spécial Casoar, n°52, 1er trimestre 1999.
DANINO O., « La stratégie cybernétique de l'Etat d'Israël », *Sécurité Globale,* n° 2013/2, pp.15-24.
DELLA PORTA D. et MOSCA L., « Global-net for global movements ? A network of networks for a movement of movements », *Journal of public policy*, 2005, 25-1.
DIOGÈNE (revue du conseil international de la philosophie), *Persuasion et influence sociale*, n°217 Janvier 2007.
DOTCOROW C., « Cyberactivisme, Cory Doctorow répond à Evgeny Mororozov », *Readwrite*
web, 28 Janv. 2011.
DOUZET F., « Les pirates du cyberespace » in *Hérodote*, 2009-3, pp. 176-193.
ECOREV n° 37 « Réseau(x) et société de l'intelligence. Les numérique sème-t-il la révolution ? » Éditions Ecorev, 2012
ESFANDIARI G., « The Twitter Devolution », *Foreign Policy*, 7 juin 2010.
FORTAT V. et KEMPF O., « Cyberstratégie chinoise : du contrôle à l'expansion », *AGIR, revue de la société de stratégie*, octobre 2013.
HORIZONS STRATÉGIQUES « Les nouveaux défis dee la mondialisation », CSFRS, 2012

HUYGHE F.B. (dir.), « L'information, c'est la guerre », *Panoramiques* n°52, 2° trimestre 2001.
HUYGHE F.B. (dir.), « La Chine et Google, décryptage d'un conflit », *Observatoire géostratégique de l'information*, 30 mars 2010.
JARVIS J., « Gutenberg of Arabia », *Buzz machine*, 13 février 2011.
JOWET G., « Propaganda and communication: The Re-emergence of a research tradition », *Journal of communication*, Hiver 1987.
KAGAN R., « Power and Weakness », *Policy Review*, n°113, juin/juillet 2002.
KEMPF O., « Entreprise et cyberstratégie », *Nouvelle revue géopolitique*, février 2013.
KEMPF O., « Cyberstratégie à la française », *RIS* n° 87, septembre 2012.
KEMPF O., « Cadre de recherche de la cyberstratégie », *Revue Défense Nationale*, juin 2012.
KEMPF O., « L'Otan et la cyberdéfense », *Sécurité Globale* n° 19, mai 2012. *[Chaire cyberdéfense Saint-Cyr, http://www.st-cyr.terre.defense.gouv.fr, mai 2013.]*
KEMPF, O. , « La cyberstratégie de l'Union Européenne », *Sécurité Globale* n° 24 (été 2013), p. 25-40.
KEMPF O., « Le cyberterrorisme : un discours plus qu'une réalité », in *Hérodote*, printemps 2014.
LIBISCKI M., « Cyberspace is not a warfighting domain », *Journal of law and Policy*, vol. 8:2, 2012.
MANRIQUE M., « Réseaux sociaux et médias d'information », in *Confluences Méditerranée*, 2011-4, pp. 81-92.
MAZZUCCHI N., « Alliance militaire et guerre économique, le cas de l'OTAN », in *Revue Défense Nationale* supplément numérique, été 2012.
MAZZUCCHI N., « L'économie, cible privilégiée de la guerre informationnelle » in *Revue Défense Nationale* n°770, mai 2014.
MAZZUCCHI N., « Conférence de Dubaï, la régulation du Net n'aura pas lieu » in *Sécurité Globale* n°24 (été 2013).
MÉDIUM (revue) *Frontières,* n° 24, 2011
MÉDIUM (revue) *Réseaux sociaux après l'utopie ?,* n° 29, 2011
MÉDIUM (revue) *Secrets à l'ère numérique*, n° 37, 2013
Monde diplomatique - Manière de voir - *Médias et contrôle des esprits et Médias, mensonges et démocraties*, hors-série 1988.
NABBALI T. et PERRY M., « Going for the Throat: Carnivore in an Echelon World, University of Western Ontario, Computer Science Department », in *Computer Law & Security Report* Vol.19 n°6, 2003.
NOUVELLE REVUE GÉOSTRATÉGIQUE, *Le Cyberespace nouvelle frontière du monde ?*, n° 8, premier trimestre 2012.
Observatoire géostratégique de l'information (Huyghe F.B., dir.), *"Facebook, Twitter, Al Jazeera et le printemps arabe", "Cyberstratégie" (1 et 2)* et *"Technologies de libération vs contrôle technologique"*, IRIS, numéros d'avril 2011 à avril 2012.
REVUE INTERNATIONALE STRATÉGIQUE (F.B. Huyghe dir.), dossier *Cyberespace : nouveaux enjeux stratégiques,* n° 87, septembre 2012.
REVUE POLITIQUE ÉTRANGÈRE., *Internet, outil de puissance*. Trimestriel, été 2012.

ROSEN J., « Prism, un défi pour le droit », Le Monde, 27 octobre 2013, http://abonnes.lemonde.fr/technologies/article/2013/10/27/espionnage-de-la-nsa-quels-recours-juridiques-pour-les-citoyens-francais_3503775_651865.html
SANG-HUN C., « South Korea Blames North for June Cyberattacks », 16 juillet 2013, http://www.nytimes.com/2013/07/17/world/asia/south-korea-blames-north-for-june-cyberattacks.html?_r=0
SOLOMON, « La financiarisation de la connaissance », in *Multitudes*, 2010-2.
SYMANTEC, « Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War », 26 juin 2013, http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war.
TISSIER G., « La nouvelle initiative de défense stratégique américaine dans le cyberespace » *Les notes stratégiques*, CEIS 2012
TRAN DAI C., « L'Internet en République populaire de Chine : vers un outil de démocratisation ou de renforcement de l'État-parti ? », Fondation pour la Recherche Stratégique, 26 janvier 2007.
WATIN-AUGOUARD G., « La LPM et la cybermenace », Observatoire du FIC, 22 octobre 2013, http://www.observatoire-fic.com/la-lpm-et-la-cybermenace-par-le-general-darmee-2s-marc-watin-augouard/
WAXMAN M.C., « Cyber Attack and the Use of Force », *The Yale Journal of International Law*, vol 36 (2011) pp 421-59

Sommaire