GRENOBLE ECOLE DE MANAGEMENT
TECHNOLOGY & INNOVATION
une école CCI GRENOBLE

CLES
Comprendre Les Enjeux Stratégiques
Note hebdomadaire d'analyse géopolitique

154
5 mars 2015

Internet, un espace de jeu géopolitique

'L'extension du domaine de la lutte' au monde numérique

Par Jean-François Fiorina
Directeur adjoint de Grenoble Ecole de Management
Directeur de l'ESC Grenoble

Le piratage massif de Sony Pictures, fin 2014, est venu rappeler l'importance de l'espace numérique pour les grandes entreprises mondialisées. Mais aussi pour les États, les Américains accusant Pyongyang d'être à l'origine de l'attaque dans un contexte de forte tension entre les deux pays. De même, la propagande essentiellement "virale" de l'État islamique souligne l'intérêt stratégique, pour toute organisation, de maîtriser son image en pratiquant ce que l'Agence pour la diffusion de l'information technologique (ADIT) nomme la "*diplomatie digitale*". Si Internet ne constitue qu'une partie du cyberespace (cf. note *CLES* n°54, 09/02/2012), il est à l'évidence un nouveau territoire où se jouent et se déploient des rapports de force tout autant économiques que politiques, symboliques et militaires. En tant que média, il est à la fois cible et vecteur de "*conflits informationnels*" qui révèlent l'acuité des jeux d'influence géopolitiques.

Mondialisation et révolution numérique sont intimement liées. Conduisent-elles à un monde nouveau, où la multiplication des échanges abolirait, au moins progressivement, toute conflictualité ? Derrière les discours, quelle réalité se joue ? Dans *Comprendre le pouvoir stratégique des médias* (Eyrolles, 2005), l'universitaire François-Bernard Huyghe souligne que "*notre époque recourt à la métaphore du réseau - souple, vivant, innovant - et l'oppose volontiers aux structures rigides, hiérarchiques, formelles de l'ère industrielle. Le Web est comparé à une toile d'araignée mondiale, un filet tendu sur la planète, dont chaque maille serait un ordinateur et chaque fil une ligne de communication. Il se développe même une véritable utopie du fonctionnement en réseau, comme si le fait de faciliter la communication - notamment celle des biens immatériels comme l'information - était en soi porteur de démocratie, d'apaisement et d'inventivité. Et comme si les réseaux excluaient le pouvoir*". L'on se souvient de l'effet d'optique et donc des erreurs d'analyse qui ont conduit à notre appréciation des "printemps arabes" : il ne suffit pas d'utiliser Facebook et Twitter, même contre une dictature, pour prétendre être un "démocrate" au sens des critères occidentaux !

Le développement d'Internet et donc de la communication n'est pas en soi porteur "de démocratie, d'apaisement et d'inventivité" : les réseaux n'excluent pas le pouvoir.

Internet, échiquier géopolitique

L'utilisation massive de la communication numérique et des réseaux sociaux par les jihadistes de Daesh est symptomatique des progrès réalisés en termes de propagande à l'ère d'Internet. Les États occidentaux ou alliés ne s'y sont pas trompés, qui tentent d'occuper le terrain par une contre-propagande institutionnelle.

Contre-offensive souvent maladroite, car l'identité et l'efficacité d'Internet tiennent précisément à son aspect transgressif, militant, non officiel. Ce qu'il est intéressant d'observer ici, c'est que pour l'État islamique, Internet est un front, un "*champ de bataille*" au même titre que les confins irakiens et syriens. La communication engagée ne vise pas la séduction ou la justification, mais pour l'essentiel l'amplification de la campagne de terreur menée sur le terrain : la diffusion des exactions commises, souvent insoutenables, est un moyen d'intimidation et d'emprise sur les populations qui se veut au moins aussi efficace que les exactions elles-mêmes. Les capacités humaines, techniques et financières qu'y consacre Daesh le prouvent amplement.

Pour l'EI, Internet n'est pas qu'un outil de communication : c'est un front supplémentaire dans son combat pour le califat.

Entreprises ou États : un enjeu stratégique

Même lorsque les cibles sont des entreprises, la logique politique n'est pas toujours loin. En témoigne la retentissante attaque informatique du 24 novembre 2014 contre Sony Pictures, considérée comme la plus importante ayant touché à ce jour une grande entreprise. En raison de sa sophistication, mais aussi de son ampleur : la quasi-totalité des fichiers présents sur le réseau de l'entreprise américaine, depuis le contenu des messageries jusqu'aux fichiers de films qui n'avaient pas encore été diffusés, a été subtilisée par les "*pirates*". Pour Washington, une telle attaque ne pouvait provenir que de la Corée du Nord. De nombreux experts, parmi lesquels les services de renseignement français, doutent de la version américaine, les preuves présentées ne suffisant pas à établir la culpabilité de Pyongyang dans ce vol de données. Mais les États-Unis ont d'ores et déjà pris des mesures de rétorsion, tandis que Sony renonçait à la diffusion du film *L'interview qui tue*, vivement dénoncé par le régime nord-coréen, et qui aurait été considéré comme le prétexte de la cyber-attaque… L'affaire a surtout permis de mettre à jour le système de surveillance de l'Agence nationale de sécurité américaine, mis en place dès 2010 : "*Conçu à l'origine comme un moyen de récolter des informations sur le programme nucléaire de ce régime ultra-secret, l'opération de la NSA a progressivement évolué au vu de la menace grandissante de la Corée du Nord en matière d'espionnage informatique, après une attaque contre des banques sud-coréennes en 2013*" (*Les Échos*, 20/01/2015).

"*Le crime sur la Toile, qu'il soit ludique, politique ou crapuleux, a connu une accélération spectaculaire ces deux dernières années*, observe le journaliste Philippe Escande dans *Le Monde* (02/02/2015). *Les dégâts sont considérables et les victimes désemparées, qu'il s'agisse d'entreprises ou de particuliers. Le piratage des données bancaires des clients du distributeur américain Target aurait coûté 1 milliard de dollars (885 millions d'euros) à l'entreprise et son poste au PDG, Gregg Steinhafel*". Quant à Sony Pictures, la divulgation des courriels de sa vice-présidente, Amy Pascal, a conduit à sa démission le 5 février 2015. "*En France, les sinistres explosent également et se chiffrent en centaines de millions d'euros.*" Deux raisons essentielles l'expliquent. D'une part, l'extension du périmètre-cible, du fait de la dématérialisation des processus métiers, de l'explosion de la mobilité, de la mise en place de nouveaux canaux de vente et de communication, etc. D'autre part, la sophistication des attaques et l'organisation en réseau des cybercriminels, capables d'exploiter au mieux les vulnérabilités des systèmes informatiques. Or les enjeux sont colossaux. Selon une étude du *Ponemon Institute* (26/05/2014), le coût total moyen d'une violation de données personnelles des clients d'une entreprise est estimé 4,16 millions d'euros, dont 2,28 millions d'euros de perte directe de chiffre d'affaires et 1,14 million d'euros de coûts induits (centre d'assistance, réparation, remises à la clientèle, etc.) - sans compter l'atteinte à l'image, devenue un actif majeur du fait même du développement de l'univers numérique ! Le sujet est devenu à l'évidence stratégique.

Qu'il soit ludique, politique ou crapuleux, le crime sur la Toile a connu une spectaculaire accélération ces deux dernières années.

Un nouvel 'Art de la Guerre' ?

Si la "*neutralité*" est au cœur du projet numérique, Internet n'est pas neutre en soi. La législation française considère ainsi les attaques cyber comme un acte de guerre, et selon *Le Monde* (04/02/2015), "*face à la redoutable influence exercée par*

le groupe État islamique (EI) dans les esprits occidentaux", l'armée française vient de mettre en place une cellule de contre-propagande sur le Net, composée d'une cinquantaine de spécialistes du Centre interarmées d'actions dans l'environnement (CIAE). D'un point de vue strictement économique, le marché mondial de la cybersécurité est en croissance annuelle de près de 8 %, et devrait atteindre 86 milliards de dollars en 2016. "*L'univers cybernétique est désormais l'un des principaux domaines de la fraude et du crime*", a déclaré un expert anglais à la suite du piratage de 233 millions de fiches clients d'un géant d'e-commerce, rapporte Xavier Raufer dans son dernier ouvrage consacré à la "*cyber-criminologie*". Le Plan cybersécurité de la nouvelle France industrielle, lancée en septembre 2013, prévoit la mise en place d'un label France des produits de cybersécurité en 2015, afin de tenter de retrouver une certaine autonomie stratégique en la matière.

En fait, Internet est foncièrement "dual". Il est *un moyen*, un outil d'influence et d'action au profit des acteurs de la mondialisation. Mais il est aussi *un espace* où se déploient les stratégies de puissance, de croissance, de prédation ou de (re)positionnement de ces acteurs. Donc un "*territoire*" au sens de l'analyse géopolitique, à savoir un "*espace habité* [même virtuellement, mais en tout cas occupé] *par les hommes, un terrain 'magique', signifiant, chargé de symboles et de mémoires concurrentes*" (Olivier Zajec, *Introduction à l'analyse géopolitique*, Argos, 2013).

Internet n'est pas qu'un outil, c'est un espace où se déploient les stratégies de puissance, donc un "territoire" au sens de l'analyse géopolitique.

Si Internet modifie en profondeur l'activité économique, nos organisations et jusqu'à nos modes de vie, l'on aurait tort de croire qu'il altère la réalité des rapports de force entre acteurs, ou même leur anthropologie. Même bousculée, c'est bien l'hyperpuissance américaine qui contrôle toujours, via l'ICANN (*Internet Corporation for Assigned Names and Numbers*), la "*gouvernance d'Internet*", et surtout l'essentiel des infrastructures physiques qui en permettent le fonctionnement. C'est-à-dire à la fois le *soft* et le *hard*. Et en tant que média, le Web modifie certes les modalités, mais pas la réalité des rivalités géostratégiques, des conflits idéologiques, identitaires, criminels ou religieux qui agitent le monde. Au mieux, il équilibre le rapport "*du fort au faible*", au profit de ce dernier. Comme le relevait déjà François-Bernard Huyghe dans *L'ennemi à l'ère numérique* (Puf, 2001), "*le conflit informationnel, révélé et amplifié par les nouvelles technologies, est né bien avant elles : les arts de combattre, d'infliger un dommage ou de gagner un avantage par des mots et des images sont aussi vieux que la stratégie, donc que l'humanité*". Il n'est donc sans doute pas près de disparaître. ■

Pour aller plus loin : "*Une stratégie pour la cybersécurité*", dossier de la *Revue de la gendarmerie nationale*, n°251, 12/2014, www.gendarmerie.interieur.gouv.fr ; *Le cyberespace : nouveau domaine de la pensée stratégique*, sous la direction de Stéphane Dossé, Olivier Kempf et Christian Malis, Economica, 2013, 192 p., 19 ☐ ; *Cyber-criminologie*, par Xavier Raufer, CNRS Editions, 2014, 240 p., 20 ☐

EXTRAIT :

Sur la nature et l'ampleur des 'écoutes' américaines : "*Nous ne sommes pas du tout dans le cas de figure où un juge d'instruction fait un mandat pour une écoute téléphonique ou une interception électronique sur une personne précise, dans une affaire précise et pour une instruction précise. Nous parlons de 'pêche au filet' pour trouver des indices suspects. Dans un cadre juridique abominablement flou (une sorte de permission générale de surveiller des gens qui pourraient être étrangers ou avoir des profils suspects), le tout avec tribunaux et procédures secrètes, la National Security Agency (NSA) peut piocher des millions de métadonnées (des données relatives aux conversations : qui a été en contact avec qui, quand et où) chez Verizon, l'opérateur téléphonique et, avec l'accord de Google, Facebook et autres grands du Net, les analystes ont, en outre, accès à des contenus : conversations, écrits, paroles (sur Skype)… Par mots clefs, ils cherchent à repérer ce que l'on nomme des 'mèmes', des unités de sens (des mots qui ont à peu près la même signification, ou des connotations suspectes) et à mettre en rapport les données pour anticiper des comportements. Toujours la confiance dans la technologie et le traitement de données ! Et toujours sans réquisition judiciaire spécifique, donc hors de toute possibilité effective de contrôle.*" (François-Bernard Huyghe, interview à *Géopolis*, magazine télévisé de France2, 11/06/2013)