Communication & Influence

N°92 - Avril 2018

Quand la réflexion accompagne l'action

Guerre informationnelle et jeux d'influence dans le cyberespace : le décryptage d'Olivier Kempf

Tout en menant une carrière militaire qui l'a conduit à devenir un fin connaisseur de l'Otan et l'un des pilotes de la transformation digitale de l'armée de Terre, Olivier Kempf a poursuivi une carrière académique : docteur en science politique, il a enseigné dans de grands établissements supérieurs (Sc. Po. Paris, HEC, Ecole de Guerre, X...) et est un expert reconnu des questions relatives au cyberespace, notamment dans sa dimension stratégique. Un cyberespace méconnu, qui est pourtant un lieu privilégié de conflictualité, tant pour les Etats que pour les entreprises.

Dans l'entretien qu'il a accordé à Bruno Racouchot, directeur de Comes Communication, Olivier Kempf dissèque les nouvelles règles qui président aux conflits dans le cyberespace où se déroule une guerre économique feutrée, mais impitoyable et bien réelle. Aussi en appelle-t-il à plus de lucidité et de réalisme pour affronter les défis qui se posent à nous. Car gérer les rapports de force informationnels dans le cyberespace est moins une question technique que d'état d'esprit. Espionnage, sabotage et subversion y règnent en maîtres dans des jeux informationnels d'une complexité sans cesse grandissante...

Existe-t-il des jeux d'influence dans le cyberespace ?

D'abord, il faut bien comprendre dans quel cadre se déploient les actions au sein du cyberespace. Ce dernier se structure en trois couches : physique, logique, sémantique. La première, physique, concerne l'ensemble des matériels de toutes sortes utilisés pour manier la donnée, l'information, et la transmettre. La seconde, logique ou logicielle, intègre l'ensemble des dispositifs de codage et de programmation qu'utilisent les machines et infrastructures afin de transformer et transférer l'information. La troisième est la couche sémantique. Elle s'intéresse au sens de l'information, étant donné que celle-ci ne peut être réduite à de la "donnée" neutre. C'est cette dernière couche, parfois dénommée couche cognitive ou couche informationnelle, qui constitue le cœur de la problématique qui nous intéresse ici.

En effet, cette couche sémantique concerne l'ensemble des données et informations qui circulent dans le cyberespace. A partir de leur exploitation, on donne de l'intelligence à ces masses de données qui deviennent de l'information. En conjuguant ces informations, en leur donnant du sens, on produit des connaissances qui vont devenir parties prenantes à des jeux de pouvoir. Il y a

Pourquoi Comes ?

En latin, comes signifie compagnon de voyage, associé, pédagogue, personne de l'escorte. Société créée en 1999, installée à Paris, Toronto et São Paulo, Comes publie chaque mois Communication & Influence. Plate-forme de réflexion, ce vecteur électronique s'efforce d'ouvrir des perspectives innovantes, à la confluence des problématiques de communication classique et de la mise en œuvre des stratégies d'influence. Un tel outil s'adresse prioritairement aux managers en charge de la stratégie générale de l'entreprise, ainsi qu'aux communicants soucieux d'ouvrir de nouvelles pistes d'action.

Être crédible exige de dire clairement où l'on va, de le faire savoir et de donner des repères. Les intérêts qui conditionnent les rivalités économiques d'aujourd'hui ne reposent pas seulement sur des paramètres d'ordre commercial ou financier. Ils doivent également intégrer des variables culturelles, sociétales, bref des idées et des représentations du monde. C'est à ce carrefour entre élaboration des stratégies d'influence et prise en compte des enjeux de la compétition économique que se déploie la démarche stratégique proposée par Comes.

COMES

www.comes-communication.com

donc en permanence au sein de ce cyberespace des jeux d'instrumentalisation des données et des informations, qui servent des intérêts et donc alimentent des conflictualités. Et l'essentiel de ces conflictualités, entre Etats bien sûr mais aussi entre entreprises, se déploie sur la couche dite informationnelle.

A cet égard, il faut bien comprendre que l'on est passé d'un monde de concurrence et de compétition à un monde de conflictualité et de guerre économique, où la guerre de l'information joue un rôle majeur. Je dois confesser que j'ai longtemps été rétif à cette expression de "guerre économique", qui me paraissait excessive. Mais l'on doit bien reconnaître que, dès la décennie 1990-2000, on assiste à des affrontements où des acteurs hétérogènes (entreprises et États) s'allient afin de faire valoir des intérêts simultanément publics et privés. Les catégories classiques sont bouleversées de fond en comble. On voit ainsi de plus en plus intervenir les autorités publiques sur un mode direct ou feutré, afin de soutenir et faire gagner "leurs" entreprises.

S'efface un autre paramètre, à savoir la séparation entre le public et le privé. Pour preuve, aux Etats-Unis, l'interaction profonde et mutuellement profitable entre les services de renseignement et les grands acteurs du cyber. La NSA surveille certes les terroristes, mais l'essentiel de son activité concerne le renseignement économique.

La guerre informationnelle fait donc pleinement partie de la guerre économique, a fortiori dans le cyberespace…

Indéniablement. Le grand processus de mondialisation des années 1990 a été permis par l'éclosion des technologies de l'information et de la communication. Le paradigme de la "concurrence pure et parfaite" – si tant est qu'il ait d'ailleurs jamais existé – s'évanouit dans le cyberespace pour faire face à la conflictualité permanente et omniprésente. De même que s'efface un autre paramètre, à savoir la séparation entre le public et le privé. Pour preuve, aux Etats-Unis, l'interaction profonde et mutuellement profitable entre les services de renseignement et les grands acteurs du cyber. La NSA surveille certes les terroristes, mais l'essentiel de son activité concerne le renseignement économique. De même, la Chine a déployé un formidable dispositif cyber centré sur l'espionnage économique. Pourquoi ? Parce que par ce biais, la Chine compte renforcer sa souveraineté et permettre l'émergence de sa puissance. Ces deux superpuissances ont une pleine conscience de l'interaction entre public et privé.

On peut distinguer trois types majeurs d'agression dans cette guerre informationnelle. La guerre pour l'information équivaut à de l'espionnage. La guerre contre l'information correspond au sabotage. La guerre par l'information est assimilée à de la subversion.

Il faut en outre bien appréhender l'ampleur et la nouveauté du phénomène auquel nous nous trouvons confrontés. La mondialisation et la révolution du cyber qui la favorise et l'accompagne sont de formidables instruments de dissolution des structures. On évoque souvent les ravages de la corruption, mais celle-ci n'est que la conséquence dans l'aire économique de la dissolution des structures existantes. On observe ainsi un affaiblissement des Etats et en corollaire, le retour d'hommes forts à leur tête, tentant de contrer cette tendance générale. Car il existe bel et bien une demande émanant des populations du monde entier, de retour aux structures établies et à un ordre commun qui permette d'endiguer la fluidification générale et de revenir à une stabilité dont les peuples ont la nostalgie.

Quels sont les risques majeurs sur le plan informationnel pour une entreprise dans le cyberespace ?

On peut distinguer trois types majeurs d'agression dans cette guerre informationnelle. La guerre pour l'information équivaut à de l'espionnage. La guerre contre l'information correspond au sabotage. La guerre par l'information est assimilée à de la subversion.

Premier cas, l'espionnage : il vise à acquérir les informations sensibles de l'entreprise, sur son fonctionnement interne (organisation, finances…) ou sa stratégie externe (axes de développement, campagnes marketing à venir…). Second cas, le sabotage. Il va tendre à perturber voire corrompre le dispositif-cible. L'attaque peut être d'ordre technique ou aller plus loin, pouvant salir ou détruire la notoriété de la structure visée, en attaquant son image de marque, autrement dit en dévalorisant son capital immatériel. On entre ici dans le troisième type de menace évoqué, à savoir la subversion. Dès lors, nous ne sommes plus dans le simple domaine de l'e-réputation, mais bien dans une sphère autre, celle de l'utilisation de toutes les ressources du cyberespace dans la guerre informationnelle que se livrent les entreprises.

Alors que faire ?

Poursuivre et amplifier la démarche initiée par l'intelligence économique en la transformant en intelligence stratégique. Si l'intelligence économique consiste en l'utilisation de techniques de renseignement, de veille, d'influence au profit des entreprises, l'intelligence stratégique, elle, constitue l'étape d'après, celle qui intègre pleinement cette dimension supplémentaire amenée par la mondialisation et le digital que nous venons d'évoquer. Tous les champs sont désormais ouverts, mais dans une configuration de conflictualité généralisée, avec des kyrielles d'acteurs publics et privés, officiels et non-officiels, avec des jeux relationnels et de pouvoirs qui ne se situent pas dans le cadre d'organigrammes classiques, mais n'en sont pas moins bien réels. L'intelligence stratégique a dès lors pour but d'identifier les forces qui sont réellement à l'œuvre derrière le paravent des institutions et d'en saisir le fonctionnement. Pour ma part, en tant que stratégiste, j'aide les entreprises à prendre conscience de ces nouveaux défis, à comprendre la nature des jeux de puissance et d'influence qui se déroulent dans ces conflictualités d'un nouveau genre, et enfin, à décider. ■

EXTRAITS

Cyberespace et intelligence économique : l'entreprise face aux nouveaux défis informationnels

Fin 2015, Olivier Kempf et Nicolas Mazzucchi – docteur en géographie économique, alors chercheur à l'IRSEM et à l'IRIS, aujourd'hui à la FRS – publient un article intitulé Cyberespace et intelligence économique *dans la revue* Géoéconomie *de l'Institut Choiseul (n°77). Selon eux,* "l'intelligence économique se révèle, par ses méthodologies et son approche particulière de l'information, un parfait cadre d'adaptation à un environnement économique où la donnée devient la nouvelle richesse." *En lisant les lignes qui suivent, on mesure à quelle vitesse les choses ont évolué...*

Fluidité et sécurité des flux d'informations

"L'intelligence économique vise, au travers de l'information, tant à protéger qu'à accroître le patrimoine de l'entreprise. Pour ce faire l'information doit être repositionnée dans le contexte plus global des trois couches du cyberespace car si la couche sémantique s'avère centrale, elle prend nécessairement appui sur les deux autres.

"L'articulation des systèmes d'information de l'entreprise, surtout dans le cas des firmes transnationales, se révèle particulièrement complexe et nécessite de disposer de fonctions dédiées. Outre la DSI et les RSSI chargée de la bonne marche du système en lui-même, la fonction de *knowledge management*, relevant de l'intelligence économique, gagne en importance. L'éclatement des centres de recherche, de commandement et de production des entreprises entraîne de potentielles pertes d'information le long des chaînes fonctionnelles et nécessite la mise en place de politiques internes dédiées à fluidifier sa circulation. Il s'agit ainsi de s'assurer que chacun dispose de la bonne information, de manière intégrale et au bon niveau de sécurité afin d'accomplir au mieux sa tâche. L'allongement des chaînes logistiques avec des délocalisations de centres de production vers les pays en développement induit naturellement pour les entreprises la prise en compte de ces enjeux dans leur stratégie de commercialisation. De même le recours accru à l'externalisation pour toute une série de fonctions, variant selon les secteurs et les entreprises, induit nécessairement une politique de valorisation de l'information interne avec une nécessaire circulation de cette dernière de l'intérieur vers l'extérieur et réciproquement qui n'est pas sans poser des problèmes de sécurité.

"Le recueil et la valorisation des informations, par exemple *via* le *big data*, se révèlent de plus en plus important pour les firmes. La connaissance des marchés et des clients potentiels ou habituels par le recueil de leurs données est l'un des nouveaux business des géants du Net. Google, Apple, Facebook ou Amazon sont ainsi positionnés maintenant comme prestataires des entreprises dans le but de recueillir et de valoriser le plus possible les données des clients. Face à cette stratégie des multinationales américaines comment positionner les entreprises françaises ? Il s'agit là d'une question complexe dont il n'existe pas de réponse tout prête mais à laquelle l'intelligence économique doit fortement contribuer."

L'intelligence économique au plus près de la direction stratégique de l'entreprise

"La réorganisation des entreprises autour de la donnée, telle que nous l'avons décrite, apparaît comme une nouvelle mutation qui n'atteindra tous ses effets qu'avec la volonté de valoriser l'information et la donnée. Elle s'articule autour du phénomène de Données massives (*Big Data*). Il s'agit dans ce cas d'utiliser toutes les données de l'entreprise pour trouver de nouveaux besoins, de nouvelles attentes, mais aussi de nouveaux métiers. Ceci impose de réfléchir aux données disponibles. Il ne s'agit plus simplement de regarder leurs sensibilité, comme précédemment, mais de réfléchir aux sources possibles d'information. Certaines sont propres à l'entreprise, qu'il s'agisse des données techniques, commerciales, financières, quand d'autres peuvent lui être extérieures (mention de la marque sur les réseaux sociaux, utilisation des bases de données ouvertes disponibles – *open data*).

"Si le traitement de toutes ces données est le fait de spécialistes hautement qualifiés (à la fois informaticiens de haut vol, statisticiens et bricoleurs inventifs), le RIE peut agir en soutien par sa connaissance fine de la "donnée" de l'entreprise. Comme il s'intéresse depuis longtemps au sens de la donnée, il sera un interlocuteur régulier des équipes de Données massives (généralement externalisées) car il sera un des seuls à avoir la vision aussi bien de la donnée interne de l'entreprise (celle qu'il protège) que de la donnée extérieure à l'entreprise (celle qu'il observe au travers de sa fonction veille). Il pourra ainsi déceler des tendances ou des liaisons qui seront fructueusement mises en équation par les équipes de Données massives. Il s'agit d'une évolution importante du métier de veilleur/analyste avec une composante principale qui reste certes qualitative mais avec une place de plus en plus importante faite aux aspects quantitatifs. Il se positionne ainsi en première ligne dans le traitement de l'information pour servir de support aux équipes de production et de commercialisation en aidant à l'appréhension fine des besoins des clients et des attentes du marché. La nouvelle organisation de l'entreprise autour de la donnée qu'elle soit interne ou externe contribue à recentrer les fonctions d'intelligence économique, mais aussi de DSI et de RSSI, au plus près de la direction stratégique de l'entreprise."

Pour en savoir plus sur la revue *Géoéconomie* de l'Institut Choiseul : http://choiseul.info/geoeconomie/

Pour télécharger l'article complet d'Olivier Kempf et Nicolas Mazzucchi : https://www.cairn.info/revue-geoeconomie-2015-5-p-45.htm

EXTRAITS

Véracité des informations et jeux d'influence dans le cyberespace

Fin 2017, Olivier Kempf publie Communication blanche et véracité des informations*, une analyse sur l'authentification des messages délivrés sur le Net. On voit à la lecture de cette analyse que les frontières sont ténues entre les différents types de communication, blanche, grise et noire… Ce qui complexifie encore le décryptage des jeux d'influence et des luttes informationnelles dans le cyberespace. Extraits.*

Communication blanche, grise ou noire ?

"[…] la communication est blanche, grise ou noire. La couleur résulte de deux critères : la véracité de l'information et le contrôle de sa diffusion par son auteur. Par exemple, les courriels d'Hillary Clinton étaient vrais mais elle n'a pas contrôlé leur diffusion. Une information vraie peut donc être à la source d'une communication noire. À l'inverse, une information fausse peut être diffusée tout à fait sciemment, comme dans le cas de la propagande (que celle-ci soit d'ailleurs blanche, noire ou grise) : alors la communication sera également noire. En revanche, une information vraie contrôlée par son auteur appartient au registre de la communication blanche.

"La couleur intermédiaire (grise) dépend principalement du degré de contrôle de l'information. La notion de contrôle se prête à toutes les nuances, surtout dans les conditions modernes de diffusion permises par les réseaux sociaux. Prenons ce qu'on a appelé "l'effet Streisand". La chanteuse a en effet poursuivi en justice en 2003 l'auteur d'une photographie de sa propriété privée. Or, la publication de la procédure a eu pour effet de faire connaître l'image par les internautes : beaucoup virent la photo et la relayèrent sur les comptes sociaux, au détriment de Barbara Streisand. Ainsi, en voulant contrôler une information vraie, la chanteuse a réussi à attirer l'attention sur ladite information beaucoup plus que si elle s'était tue. Au fond, on a le plus grand mal à contrôler les informations de nos jours (ou plus exactement à restreindre leur diffusion). L'effet Streisand appartient logiquement à la catégorie de la communication grise.

"Mais une information fausse peut également être peu contrôlée, comme par exemple des rumeurs de toutes sortes (remarquons qu'une information peut être faussée sans être fausse) ou des informations ne présentant qu'une partie de la vérité ou mélangeant des bouts de vérité et des bouts de mensonge. Cela peut naître spontanément sur les réseaux sociaux, par un internaute qui n'a pas la rigueur qu'on attendrait d'un journaliste chevronné, ou encore par manipulation d'un service spécialisé qui utilise des faux-nez pour lancer des rumeurs sur Internet. Là encore, on est dans la catégorie de la communication grise."

Vérifier et garantir l'information

"Constatons que l'auxiliaire humain est aujourd'hui le moyen utilisé pour atteindre cette garantie. Or, il ne donne pas satisfaction. En effet, les méthodes employées sont diverses : elles contribuent à une certaine authentification sans la garantir complètement.

"La première méthode est celle de la confiance et des signalements (systèmes de cotation de la prestation). Cette méthode est utilisée par beaucoup de plateformes d'intermédiation, par exemple AirBnB ou Blablacar. Les utilisateurs notent les prestataires. Cela est efficace à un niveau de micro échanges mais ne permet pas d'être à l'abri des surprises. En effet, le système de notation réciproque (les deux parties se notant anonymement) fait que beaucoup, dans un système de théorie des jeux, préfèrent donner une bonne note pour éviter d'en recevoir une mauvaise en retour. En effet, à donner des mauvaises notes, on se bâtit une réputation de mauvais coucheur ce qui amoindrit la clientèle.

"L'autre méthode régulièrement employée, cette fois-ci pour des informations publiques, est celle du contrôle des faits (*fact checking*) et des signatures de presse. Cela est également utile sans fournir une garantie absolue. D'une part, on ne peut pas contrôler toutes les informations et les vérifieurs sont obligés de sélectionner celles qu'ils vont vérifier : vu le nombre de déclarations publiques, ils ne nettoient qu'une part infime. Ne parlons même pas du procès en subjectivité que nous avons déjà évoqué et qui ne dit rien de la qualité de la méthode, qui seule nous intéresse ici. Quant à la signature sensée inspirer confiance, elle revient à dire qu'on fait confiance à l'expert, quel qu'il soit. Expert enquêteur (journaliste) ou expert technicien, force est de constater qu'il y a eu tellement de mélanges des genres que cela ne convainc plus aujourd'hui […]

"Dès lors, la technologie semble une voie possible. Elle seule permet d'une part de traiter la masse d'information qui est publiée chaque jour. Les chiffres sont astronomiques mais recouvrent tout et n'importe quoi et notamment toutes les photos de vacances ou égotistes publiées chaque jour sur Facebook ou Instagram. Dans le domaine des informations sérieuses, il devrait être aisé de mettre en place un système de garantie qui soit compatible avec les technologies de données de masse (Big Data), grâce aux capacités actuelles de stockage et de calcul. On peut alors imaginer deux types de systèmes. L'un qui s'attache à la véracité de l'information. Cela peut passer par l'analyse sémantique ou encore par les progrès à venir d'intelligence artificielle. Toutefois, ce *fact checking* automatique ne garantira pas à 100 % l'information traitée, sans compter les biais de subjectivité. L'autre s'attacherait au mode de diffusion et organiserait, de manière décentralisée, une diffusion de l'information garantie par l'émetteur : la combinaison de l'infonuagique (*cloud*) et de la technologie *blockchain* paraît ici envisageable."

Télécharger l'intégralité de l'analyse d'Olivier Kempf : http://www.egeablog.net/index.php?post/2017/11/23/Communication-blanche-et-v%C3%A9racit%C3%A9-des-informations

EXTRAITS

Les stratégies indirectes dans le cyberespace

Les stratégies d'influence sont le plus souvent indirectes et transverses. En ce sens, elles peuvent pleinement se déployer dans le cyberespace. Dans un article intitulé Stratégies du cyberespace *publié en février 2013 par le plus important site géopolitique francophone, Diploweb.com, Olivier Kempf met en avant le bouleversement des règles du jeu qu'implique le cyberespace en matière stratégique.*

L'opacité du cyberespace et le renouveau de la liberté de manœuvre

"La première conséquence de l'opacité est le renouveau de la liberté de manœuvre des différents acteurs. Nous vivions dans un monde stratégique marqué par la défensive, pour plusieurs raisons : morale (surtout après les catastrophes des deux guerres mondiales), juridique (selon la charte des Nations-Unies, la seule cause légitime de guerre est la légitime défense), enfin et surtout technique, à cause de la domination de l'arme nucléaire. Celle-ci a en effet opéré un bouleversement stratégique qui a interdit la montée aux extrêmes. Toute guerre envisage, en effet, l'escalade de la violence, comme l'a très tôt montré Carl von Clausewitz. Avec le nucléaire, cette escalade devenait trop dangereuse : l'un des extrêmes apparaissait tellement fatal que personne ne prenait le risque d'ouvrir la montée en entrant dans l'autre extrême, celui du déclenchement de la guerre puisque celle-ci pouvait naturellement croître jusqu'au conflit nucléaire. Ainsi, contrairement à une opinion couramment répandue, la stratégie nucléaire n'est pas une stratégie offensive, mais une stratégie fondamentalement défensive.

"L'avènement du cyberespace (lui aussi fait technologique qui vient modifier la grammaire de la guerre) provoque une nouvelle rupture stratégique. Puisqu'il est opaque, puisqu'il est non-létal, puisqu'on ne peut attribuer les actes à leurs auteurs, chacun peut "prendre l'initiative". Chacun, Etat, groupe ou individu, retrouve une liberté de manœuvre. En un mot, l'offensive redevient possible. Dès lors, les débats actuels sur son opportunité ne sont que de l'agitation médiatique : peu importe que les Etats-Unis ou Israël annoncent que leurs doctrines cyberstratégiques combinent défensive ou offensive, suivant en cela le discours précurseur et insuffisamment remarqué de la France qui, dès son Livre Blanc de 2008, annonçait son engagement dans cette direction : la nature stratégique du cyberespace, ordonnée par le principe de l'inattribution, favorise le retour de l'offensive."

Quand le cyber permet une resymétrisation de la conflictualité

"Toutefois, ce retour de l'offensive doit obéir à la contrainte de l'opacité. Ceci explique la mise en place d'une stratégie fondamentalement indirecte : Liddell-Hart et Beaufre en ont rêvé, le cyber l'a rendu possible. Voici au fond la réponse technologique aux développements asymétriques de la guerre, aux contournements récemment observés : le cyber permet de contourner le contournement des autres. Au fond, le cyber permet une sorte de resymétrisation de la conflictualité, puisque tous les acteurs vont pouvoir y opérer.

"Toutefois, il faut faire attention : on évoque parfois la capacité du hacker à infiltrer tous les systèmes informatiques. Cela a pu être le cas au cours des années 1980, mais depuis les systèmes de protection et de défense se sont durcis. On assiste ainsi à un effet de gamme, où les grands acteurs jouent dans la même division. Comme au football, si tout le monde joue le même jeu, il y a les pros qui jouent en Ligue 1 et les amateurs du dimanche : mêmes règles mais différence d'efficacité, en défense comme en attaque. Ainsi, on peut dire sans trop de risques de se tromper que les Etats-Unis, la Chine, la Russie, la France, l'Allemagne, le Royaume-Uni, Israël, l'Inde jouent en ligue 1 : et comme en ligue 1, il y a les équipes qui luttent pour le titre, d'autres de milieu de tableau, et d'autres enfin qui luttent pour éviter la relégation."

Contrairement aux apparences, le cyber se pense aussi sur le temps long

"Une autre conséquence de cette opacité est l'allongement du temps stratégique. Là encore, il faut se garder de l'illusion couramment colportée de l'instantanéité du cyber. A bien y regarder, on s'aperçoit que les actions dans le cyber nécessitent une préparation et une anticipation, d'autant plus longue que la cible est durcie. L'opération Olympic Games, qui visait à mettre en place le virus Stuxnet au sein de la centrale nucléaire iranienne de Natanz, fut décidée en 2006 : le virus mit trois ans avant d'être fabriqué et introduit dans la centrale (par une complicité humaine) et il opéra (de façon cachée) pendant un an avant que les Iraniens ne se rendent compte des dégâts. Au total, l'opération a duré quatre ans ! En fait, tout se passe comme si l'opacité permettait aussi d'échapper à l'accélération du temps que nous vivons collectivement et qui est d'ailleurs rendue possible par le développement de ce même cyberespace !

"Remarquons enfin, pour conclure ce tableau trop bref, que la cyberconflictualité est duale : s'il peut y avoir des conflits uniquement cyber (c'est l'exemple de Stuxnet), il faut constater que le cyber recoupe d'autres conflictualités : aussi bien les guerres classiques existantes (cas du raid israélien contre la Syrie en 2007, cas des réactions talibanes en Afghanistan) que les conflits politiques qui font la une de l'actualité. Ainsi, et même si les médias en parlent peu, les conflits cyber font en ce moment rage au Proche et au Moyen Orient, et recoupent toutes les lignes de conflit existantes |…] Et cette guerre recoupe une autre conflictualité, celle de la guerre économique : ainsi, on attaque la bourse de Tel–Aviv, les banques du Liban, la société pétrolière saoudienne Aramco…. Le cyber permet un mélange des genres incroyable, virulent et discret. Il est l'espace d'un néo-hobbésisme, celui de la lutte de tous contre tous"…

Pour télécharger l'article dans son intégralité : https://www.diploweb.com/Strategie-du-cyberespace.html

BIOGRAPHIE

Né en 1963, Olivier Kempf a d'abord mené une carrière militaire. Saint-Cyrien, breveté de l'école de guerre, il a alterné les temps opérationnels en régiment et en opération extérieure (Koweït, ex-Yougoslavie, Côte d'Ivoire, Tchad), une carrière internationale (plus de sept ans à l'étranger) et une carrière en état-major, toujours à des fonctions stratégiques. Il a notamment participé à la transformation de l'OTAN en 2002 comme responsable de l'Europe du sud, il a ensuite écrit le Plan stratégique des Armées en 2011, puis conseillé trois ans le Secrétaire général de l'OTAN à la tête d'une cellule d'anticipation stratégique avant d'être aujourd'hui à l'état-major de l'armée de Terre où il a rédigé la politique de cyberdéfense tout en ayant initié et conduit la Transformation digitale de l'armée de Terre. Il quitte cet été le service actif comme général de brigade.

Simultanément, il a mené une carrière académique. Docteur en science politique, titulaire d'un DEA de sciences économiques, il a publié une dizaine d'ouvrages, notamment sur la cyberstratégie dont il est un des spécialistes français reconnus, et publié plus de cent articles dans des revues académiques françaises et étrangères (*Revue défense nationale, Ramsès, Revue Internationale et Stratégique, Politique Etrangère, Limes, Stratégique, Revue de géopolitique, DSI,* …). Ses travaux portent sur la géopolitique, la stratégie et la cyberstratégie, l'intelligence économique et stratégique, le commandement et le management. Il a enseigné dans de nombreux établissements supérieurs (Science-Po Paris, HEC, Ecole de Guerre, IEP Lille, Ecole de Guerre Economique, Polytechnique) et intervient régulièrement dans des conférences, colloques ou médias (France Inter, France Culture, RFI, France 24 …). Il dirige la collection Cyberstratégie chez Economica.

Il a fondé en 2014 avec l'Amiral (2S) Jean Dufourcq La Vigie (www.lettrevigie.com), lettre d'analyse destinée aux décideurs qui propose tous les 15 jours une lecture stratégique de deux thèmes choisis. La Vigie est devenue depuis un cabinet offrant diverses prestations à ses clients (études, formations, événements).

Il vient enfin de créer son activité de consultant spécialisé en stratégie cyber, transformation digitale et intelligence stratégique. Ayant conseillé de hauts dirigeants depuis plus de dix ans, il sait en effet comprendre leurs interrogations et leur donner, dans un langage compréhensible qui est rarement le fait des spécialistes de l'informatique, les clés de la décision pour leurs organisations. Il procure ainsi de la clarté stratégique dans ces matières digitales qui sont aujourd'hui souvent obscures et perçues comme des centres de coût alors qu'une vision éclairée permet de les transformer en centres de profit. Ayant mis à jour le lien entre la révolution digitale et la guerre économique, il aide à construire les stratégies adaptées pour gagner.

Pour en savoir plus : www.olivierkempf.com

L'INFLUENCE, UNE NOUVELLE FAÇON DE PENSER LA COMMUNICATION DANS LA GUERRE ECONOMIQUE

"Qu'est-ce qu'être influent sinon détenir la capacité à peser sur l'évolution des situations ? L'influence n'est pas l'illusion. Elle en est même l'antithèse. Elle est une manifestation de la puissance. Elle plonge ses racines dans une certaine approche du réel, elle se vit à travers une manière d'être-au-monde. Le cœur d'une stratégie d'influence digne de ce nom réside très clairement en une identité finement ciselée, puis nettement assumée. Une succession de "coups médiatiques", la gestion habile d'un carnet d'adresses, la mise en œuvre de vecteurs audacieux ne valent que s'ils sont sous-tendus par une ligne stratégique claire, fruit de la réflexion engagée sur l'identité. Autant dire qu'une stratégie d'influence implique un fort travail de clarification en amont des processus de décision, au niveau de la direction générale ou de la direction de la stratégie. Une telle démarche demande tout à la fois de la lucidité et du courage. Car revendiquer une identité propre exige que l'on accepte d'être différent des autres, de choisir ses valeurs propres, d'articuler ses idées selon un mode correspondant à une logique intime et authentique. Après des décennies de superficialité revient le temps du structuré et du profond. En temps de crise, on veut du solide. Et l'on perçoit aujourd'hui les prémices de ce retournement.

"L'influence mérite d'être pensée à l'image d'un arbre. Voir ses branches se tendre vers le ciel ne doit pas faire oublier le travail effectué par les racines dans les entrailles de la terre. Si elle veut être forte et cohérente, une stratégie d'influence doit se déployer à partir d'une réflexion sur l'identité de la structure concernée, et être étayée par un discours haut de gamme. L'influence ne peut utilement porter ses fruits que si elle est à même de se répercuter à travers des messages structurés, logiques, harmonieux, prouvant la capacité de la direction à voir loin et sur le long terme. Top managers, communicants, stratèges civils et militaires, experts et universitaires doivent croiser leurs savoir-faire. Dans un monde en réseau, l'échange des connaissances, la capacité à s'adapter aux nouvelles configurations et la volonté d'affirmer son identité propre constituent des clés maîtresses du succès".

Ce texte a été écrit lors du lancement de *Communication & Influence* en juillet 2008. Il nous sert désormais de référence pour donner de l'influence une définition allant bien au-delà de ses aspects négatifs, auxquels elle se trouve trop souvent cantonnée. L'entretien que nous a accordé Olivier Kempf va clairement dans le même sens. Qu'il soit ici remercié de sa contribution aux débats que propose, mois après mois, notre plate-forme de réflexion.

Bruno Racouchot
Directeur de Comes

COMES
Quand la réflexion accompagne l'action

Communication & Influence
UNE PUBLICATION DU CABINET COMES
Paris ■ Toronto ■ São Paulo
Directrice de la publication : Sophie Vieillard
Illustrations : Rossana

CONTACTS
France (Paris) : +33 (0)1 47 09 36 99
North America (Toronto) : +00 (1) 416 845 21 09
South America (São Paulo) : + 00 (55) 11 8354 3139
www.comes-communication.com

N° ISNN 1760-4842