diploweb.com La revue géopolitique
ISSN : 2111-4307

Gagner les cyberconflits, au-delà du technique

samedi 25 juin 2016,par François-Bernard HUYGHE , Maxime ARQUILLIERE, Olivier KEMPF, Yann DERRIENNIC

Citer cet article / To cite this version :
François-Bernard HUYGHE , Maxime ARQUILLIERE, Olivier KEMPF, Yann DERRIENNIC, **Gagner les cyberconflits, au-delà du technique**, *Diploweb.com : la revue géopolitique, 25 juin 2016.*

Cet entretien exclusif fait un vaste tour d'horizon des problématiques stratégiques et géopolitiques des cyberconflits. Afin d'offrir à chacun les clés de lecture des nouveaux enjeux. Avec le cyber, le monde a changé, encore faut-il disposer des éléments nécessaires pour en prendre la mesure. Les voici.

Yann Derriennic (Y. D.) et Maxime Arquillière (M. A.) : Pour commencer, pouvez-vous expliquer comment vous en êtes venus à l'étude de la cyberstratégie ?

François-Bernard Huyghe (F.-B. H.) : Mon intérêt pour les questions cyber est ancien puisqu'en 2001, j'avais écrit *L'ennemi à l'ère numérique* pour réfléchir sur les potentialités conflictuelles d'Internet. Il y a trois ans, dans le cadre d'un appel d'offre du Conseil Supérieur de la Formation et de la Recherche Stratégiques (CSFRS), nous avons travaillé, avec le colonel Olivier Kempf et Nicolas Mazzucchi, sur la cyberstratégie dans l'optique française. Les conflits dans le cyberespace ont pour cible ultime le cerveau humain : elles visent à produire un effet de croyance et/ou à agir sur des forces "spirituelles" au sens de Clausewitz dans *De la guerre*. Attaquer peut servir à faire disparaître physiquement un adversaire – ce qui ne s'est jamais produit pour l'instant pour le cyber : personne n'est mort d'une cyberattaque – il s'agit surtout de faire céder la cible : la tromper, l'affaiblir, voire le faire adhérer à une idéologie ; toutes sortes d'actions que l'on peut mener à travers le cyber produisent un effet symbolique et psychique.

Y. D. & M. A. : Pouvez-vous nous expliquer l'objectif de ce livre ? A quel type de public s'adresse-t-il ?

F.-B. H. : Nous avons essayé de développer des catégories et une méthodologie simples. Nous nous sommes placés d'abord du point de vue de l'attaquant, afin de comprendre ses objectifs, ses voies et moyens. Ensuite, nous nous sommes intéressés à ce qui se passe une fois que l'attaque est lancée, quelles différences il y a entre l'effet réel et le modèle théorique de la cyberattaque. Enfin, nous nous sommes demandés si la victime comprend bien pourquoi elle est frappée, par qui, comment elle interprète et réagit. En somme, quels sont les effets réels de cette attaque.

Nous préconisions de dépasser une vision défensive et techniciste de la cyberstratégie. Une vision défensive réduit tout en termes de cybersécurité, protection, résilience, etc., ce que nous pensons être une erreur. Avoir une forteresse n'est pas gagner la guerre : vous n'avez pas d'anticipation ni de projets à long terme. Vous vous contenterez d'attendre la prochaine agression. Ensuite, une vision technique ignore les intentions politiques ou idéologiques derrière les offensives contre des systèmes donc leur logique. Cet ouvrage s'adresse en priorité à des personnes concernées par la cybersécurité et la cyberstratégie mais nous souhaitons toucher au-delà de ce lectorat un public de décideurs politiques ou économiques qui ont besoin d'une vision à plus long terme de ce qu'est la cyberstratégie.

Y. D. & M. A. : Dans votre ouvrage, vous parlez du cyberespace comme d'un espace complexe en trois couches. Pouvez-vous développer ces distinctions ?

F.-B. H. : Cette division n'est pas notre création, elle est devenue canonique (des chercheurs comme David Clark en parlent dès 2010). Elle reflète une réalité bien que le terme «

cyberespace » soit né dans un contexte de science-fiction, dans le roman *Neuromancien* écrit par William Gibson en 1984 pour décrire un espace surgissant de la rencontre de toutes les productions numériques.

D'abord, il y a une couche physique. Nous avons des machines que nous utilisons sur un territoire, grâce à des fournisseurs d'accès, le tout relié aux dorsales d'Internet, dont nous savons désormais que la NSA et d'autres entités peuvent extraire de l'information : tout cela est physique. Ainsi, dans le cyberespace les frontières n'ont pas disparu comme le voulaient les pionniers de l'informatique.

Pour que cette première couche fonctionne, il faut une couche logique (ou logicielle) composée de codes informatiques. Cela crée un système déterminant au sens où le code (technique) est la loi (de l'usage possible). Celui qui maîtrise le système de code (non seulement l'utilisation des codes mais leur définition et leur régulation) détient un pouvoir dominant sur l'ensemble des autres acteurs. Ainsi, les djihadistes utilisent beaucoup pour communiquer l'application Telegram (NDLR, créée à Berlin par des Russes anti-Poutine), qui permet un haut niveau d'encodage des messages. La couche logique permet aussi aux puissances de révéler leur niveau technique, leur capacité de dominer une partie du cyberespace. Si vous êtes la Chine et possédez votre équivalent national de Google, vous n'exercez pas le même pouvoir que si vous êtes un plus petit pays, auquel cas vous utiliserez des réseaugiciels – comme Google, Facebook, Twitter – gérés aux Etats-Unis.

Enfin, il y a une troisième dimension : la couche sémantique. Tout ce que nous avons décrit aboutit sur des écrans : des signes, des images, de la musique, c'est-à-dire des éléments de sens agissant sur l'esprit. C'est le principal sujet du livre car cette couche sémantique (ou informationnelle) a fait l'objet de très peu d'études.

Y. D. & M. A. : Quels sont les acteurs qui s'affrontent dans le cyberespace et quelles sont leurs spécificités ?

F.-B. H. : Longtemps, mener une attaque d'une certaine importance avec des armes fut un monopole étatique ou alors on se battait dans le cadre d'une guerre civile. Désormais, vous et moi nous pourrions, en acquérant de simples connaissances techniques, lancer des attaques numériques. Les acteurs étatiques et leurs services lancent des offensives contre d'autres Etats ou des acteurs privés. Par exemple, les Etats-Unis ont développé le logiciel Stuxnet dont le but était de mettre en panne une chaîne d'enrichissement de l'uranium pour empêcher l'Iran d'accéder à la bombe atomique.

Pour les acteurs économiques s'ouvre le champ de l'espionnage. Comme conséquence à cela apparaît la figure du mercenaire moderne : vous pouvez "louer" des moyens de cyberattaque. Au XVIème siècle, dans certains pays, la majorité des soldats étaient des mercenaires. Aujourd'hui, un acteur privé peut engager des mercenaires qui ont une capacité de nuisance et peuvent fournir la technologie nécessaire à une attaque.

Y. D. & M. A. : Ces groupes mercenaires sont-ils utilisés par les djihadistes ?

F.-B. H. : Gros problème : déterminer l'origine de l'attaque. Le "sabotage" mené par écran interposé contre la chaîne de télévision internationale *TV5 Monde* en 2015 a produit un écran

noir. Elle a été revendiquée par un prétendu « cybercalifat », mais la vraisemblance semble faible. Ceux qui ont analysé le *modus operandi* en ont souvent conclu qu'elle avait peut-être été conduite par un groupe mercenaire russe qui aurait loué sa capacité de nuisance ou d'espionnage. Cela ne signifie pas forcément commandités par le gouvernement russe, peut-être seulement tolérés. Mais qui est le vrai commanditaire ? Et quel est le message délivré ? Cela complique la réflexion stratégique en termes de riposte par les Etats à une attaque, par des moyens cyber (armes offensives) ou non. La France en possède et ils sont gérés par des services secrets, ce qui, par définition, empêche l'ennemi de savoir quel type d'arme on possède. Encore faudrait-il être sûr de frapper le bon coupable ou de dissuader le bon agresseur (éventuel).

Y. D. & M. A. : Selon vous, comment peut-on évaluer le succès ou l'échec d'une cyberattaque ?

F.-B. H. : Un des fondements de la stratégie, c'est qu'une attaque est destinée à contribuer à une victoire. Une cyberattaque passe par un réseau numérique : l'intention offensive va se traduire par des algorithmes qui vont permettre d'attaquer de trois façons.

Le premier type d'attaque sert à violer des secrets, c'est-à-dire franchir des systèmes de protection pour faire de l'espionnage. Cela inclut la surveillance (voire les révélations d'Edward Snowden) : la NSA cherche à collecter des informations sur des terroristes mais aussi à voler des informations stratégiques pour assurer la sécurité et la puissance américaines.

La deuxième manière d'attaquer correspond au sabotage : empêcher quelque chose (une machine dépendant d'un système informatique par exemple) de fonctionner. Dans le cadre de Stuxnet, les centrifugeuses vont mal fonctionner sans signes visibles. Dans le cas de *TV5 Monde*, c'est un écran noir. Imaginez les déclinaisons militaires.

Le troisième type d'attaque est rangé dans la catégorie de la "subversion". Il s'agit d'attaques à fins psychologiques destinées à provoquer un impact public (humilier la victime, la dénoncer, lancer des slogans vengeurs, etc.). Elles combinent la recherche d'un effet de sens et des compétences techniques. Ainsi, dans une attaque dite de "défacement", où vous apposez votre texte et votre image sur la page d'accueil du site d'une autorité adverse, il faut être capable d'aller sur le site de l'adversaire et de prendre le contrôle de certaines fonctions.

Olivier Kempf (O. K.) : Le succès d'une attaque dépend finalement de l'intention initiale de l'agresseur. Reprenons les trois cas évoqués par F.-B. Huyghe. Dans un cas d'espionnage, tant que ça n'est pas su, l'attaquant est victorieux et cela devient un échec dès que c'est su. S'il s'agit de sabotage, l'attaquant peut vouloir le révéler ou non et tout dépend de l'intensité des dommages qu'il veut faire. Enfin, l'attaque de subversion peut être couplée aux deux premières, où le but du jeu est surtout de faire savoir que l'on a attaqué. C'est par exemple ce qu'a fait l'armée électronique syrienne, fidèle au régime de Bachar el-Assad, en piratant le compte Twitter d'*Associated Press* (*AP*) pour publier un tweet déclarant : « *Breaking : Two explosions in the White House and Barack Obama is injured* ». Cela a eu pour effet de faire baisser l'indice boursier de New York de 10 à 15% dans les deux minutes, c'est-à-dire le temps qu'il a fallu à *AP* pour lancer un tweet de dénonciation de la fausse publication. Le but était de faire valoir l'armée électronique syrienne pour montrer que les « pro-Assad » étaient assez

puissants. Cette affaire intervenait à un tournant du conflit puisqu'au printemps 2013, l'opinion comprenait que la rébellion ne gagnerait pas et que Bachar el-Assad allait durer. Cette revendication est allée cristalliser quelque chose qui se passait sur le terrain.

Y. D. & M. A. : Vous expliquez aussi dans le livre que les frontières entre les trois types d'attaques que vous venez d'évoquer deviennent floues dans le cyberespace. Pourquoi ?

F.-B. H. : De l'espionnage reste de l'espionnage dans ses finalités (savoir) mais cela peut requérir préalablement un peu de sabotage pour perturber certaines défenses dans un système. De même, si vous sabotez, c'est que vous avez un peu espionné avant pour pouvoir surmonter des protections. Dans la pratique, les trois se mêlent mais les catégories restent toujours valables : le but principal reste de voler de l'information pour gagner en puissance, d'affaiblir même temporairement l'adversaire en lui ôtant de la capacité et produire un effet psychologique. Les deux dernières étant certes liées : pas de sabotage qui ne produise pas d'effet psychologique.

Y. D. & M. A. : Peut-on transposer les paradigmes stratégiques de la guerre conventionnelle dans le cyberespace ?

F.-B. H. : Oui et non. Oui, dans la logique française : nous ne disons pas quel type d'armes informatiques offensives nous possédons. Nous faisons le pari qu'un éventuel attaquant va considérer notre bon niveau technologique et notre « posture », comme disent les militaires, et que cela le découragera de peur de la rétorsion que nous exercerions. On est dans un raisonnement classique de dissuasion, comme dans une logique de Guerre froide.

Pour la guerre dans le cyberespace, c'est différent, on sait moins avec qui dialoguer. Evidemment il y a des suspects habituels, et nombre d'agences gouvernementales américaines désignent systématiquement la Russie et la Chine. L'art de deviner, d'évaluer, est donc crucial, en espérant, si l'on est victime d'une attaque grave, ne pas se faire tromper par un « faux drapeau ». On pense à l'affaire « Octobre rouge » signalée en 2012 où l'on a d'abord pensé à des Russes avant de s'interroger sur la présence de Chinois, peut-être commanditaires de cet espionnage. Le secrétaire général de l'OTAN a déclaré qu'une attaque cyber d'une certaine gravité pourrait déclencher une riposte avec des armes conventionnelles. Mieux vaut donc ne pas se tromper avant de lancer ses missiles.

Si je pousse ce raisonnement à l'absurde, un virus informatique peut déclencher la Troisième Guerre mondiale. Prenons un exemple en Estonie, en 2007. Le pays a subi une attaque qui a paralysé des structures étatiques après un incident d'ordre symbolique : le retrait de la statue d'un héros de l'Armée rouge. L'attaque a été menée par déni de service, c'est-à-dire que l'on attaque des pages superficielles publiques, ce qui a causé peu de dommages matériels et n'a tué personne. En revanche, l'Estonie a déclaré à l'OTAN « avoir subi une attaque comparable à une agression militaire ». Si évidemment l'OTAN n'a pas riposté en envoyant des bombardiers, l'affaire estonienne a déclenché une prise de conscience de la part des Occidentaux. Ainsi, l'Alliance a pris des mesures successives jusqu'à déclarer au sommet de Galles (2014) qu'une cyberattaque pourrait, le cas échéant, entrer sous le prisme de l'article 5 (clause de défense collective). Cette attaque constitue la première démonstration publique qu'un Etat peut exercer une pression, un dommage, une rétorsion sur un autre Etat, ce qui pourrait devenir un

déterminant des futurs conflits. Néanmoins, il faut distinguer : vous pouvez utiliser du cyber dans un conflit, c'est déjà répandu, mais le cyber "remplaçant" la guerre, semble moins crédible, pour toutes les raisons d'attribution et de revendication. On attend la très grande attaque cyber, qui produirait des morts ou la paralysie d'un pays. Pour résumer, ces attaques offensives font perdre du temps mais ne provoquent pas – encore – de dommages physiques majeurs.

Y. D. & M. A. : Est-ce en raison de la complexité du domaine que, selon vos mots, il y a un risque « d'instrumentalisation des termes et de dramatisation des menaces » de la part de certains acteurs ?

F.-B. H. : Oui, le problème c'est que la gravité du dommage, son intentionnalité et son auteur sont trois facteurs qui ne sont jamais totalement démontrés, et sur lesquels on peut mentir ou exagérer.

O. K. : Notre travail d'analyste est justement d'essayer de catégoriser, alors que l'intérêt des acteurs est de garder le flou afin de favoriser leur action. Le seul emploi des mots est significatif. Nous parlons de cyberattaque, mais je suis toujours réservé par rapport à l'utilisation du mot « attaque » qui est un terme très militaire. On n'a quasiment aucun exemple de mort causé par une cyberattaque. Le critère de létalité est, pour nous stratégistes, l'alpha et l'oméga de notre analyse des rapports guerriers. Je préfère donc le mot de cyberagression.

Entre la présidence de Nicolas Sarkozy et celle de François Hollande, il a été dévoilé que les serveurs de l'Elysée ont subi un piratage. L'Etat a attendu six semaines avant d'en parler. Pendant plus d'un an, les Chinois puis les Etats-Unis ont été suspectés avant que la piste d'un piratage par les services israéliens ne devienne la plus fiable. Dans cette affaire, rien n'a jamais été officiel, le flou est donc instrumentalisé par tous [1].

Y. D. & M. A. : Vous dites qu'à la différence des alliances traditionnelles, les alliances dans le cyberespace mettent davantage en commun les faiblesses que les forces. Pouvez-vous expliquer ?

O. K. : La caractéristique essentielle du cyberespace est son flou d'une part, son opacité d'autre part. On pense que le cyberespace est transparent et technique mais en fait, il est assez simple d'y intervenir de façon camouflée. Pour reprendre l'exemple de l'Elysée, on n'est jamais sûr de qui est l'agresseur. Dans le monde conflictuel traditionnel, on peut compter des chars qui constituent des signes tangibles d'une activité et permettent de l'objectiver. Dans le cyberespace, nous ne sommes pas capables par l'observation d'objectiver ce que font les différents acteurs, c'est opaque. Les calculs d'alliances sont donc plus difficiles à faire et nous sommes rapidement dans un système néo-hobbesien de guerre de tous contre tous. En revanche, si vous entrez en relation d'alliance avec un individu, il va falloir que vous lui ouvriez en partie vos secrets et qu'il fasse de même. Vous lui donnez donc une information qui vous affaiblit. Le système d'alliances dans le cyberespace est donc d'abord un partage des faiblesses dont on espère qu'il débouchera sur une addition des forces. Une alliance traditionnelle ne passe pas par ce partage des faiblesses mais va directement à l'addition de ressources.

Y. D. & M. A. : Qu'en est-il du transfert de technologies dans le cadre d'une alliance ?

F.-B. H. : Partager les armes offensives est encore un autre débat qui n'est, semble-t-il, pas prêt d'être ouvert. Si vous partagez une arme offensive, vous partagez une technologie avec pour risque d'affaiblir l'arme que vous possédez. Pour les moyens défensifs, il peut y avoir de la coopération dans une certaine mesure, mais c'est dans le domaine du renseignement que les alliances restent les plus intéressantes.

O. K. : La cyberdéfense peut s'articuler en trois postures tactiques principales.

La première est la protection ou « pure défense » (cyberprotection, sécurité des systèmes d'information), où sans partager des technologies, on peut réfléchir sur les schémas de protection de manière comparée.

La deuxième est la cyberdéfense active. On recherche une connaissance commune sur l'extérieur pour être au courant des activités se déroulant dans le cybermonde.

La troisième est la coopération offensive pour laquelle on a peu d'exemples. On peut simplement évoquer la coopération entre Israël et les États-Unis dans l'affaire Stuxnet. C'est intéressant car cela pose la question de la réplique d'alliances géopolitiques dans le cyber. De ce point de vue, les alliances sont très claires entre les Etats-Unis et le Royaume-Uni avec l'affaire Tempora ou l'affaire Belgacom, où les Anglais ont probablement espionné et piraté les institutions européennes pour le compte des Etats-Unis. De plus, il y a des alliances hybrides entre des Etats et des acteurs individuels comme des groupes de hackers, sous le terme de « consultance ». Cela renvoie encore aux caractéristiques du cyberespace : flou et opacité.

Y. D. & M. A. : Quelles sont selon vous les prochaines ruptures technologiques qui entraîneront des changements majeurs dans la nature et la conduite des conflits ?

F.-B. H. : Entre le *Big Data* et les objets connectés, il y aura forcément des vulnérabilités et donc des options stratégiques.

O. K. : En effet, le *Big Data* et le *cloud* vont modifier les façons de faire des armées, ce qui créera des forces et des faiblesses, comme tout changement technologique.

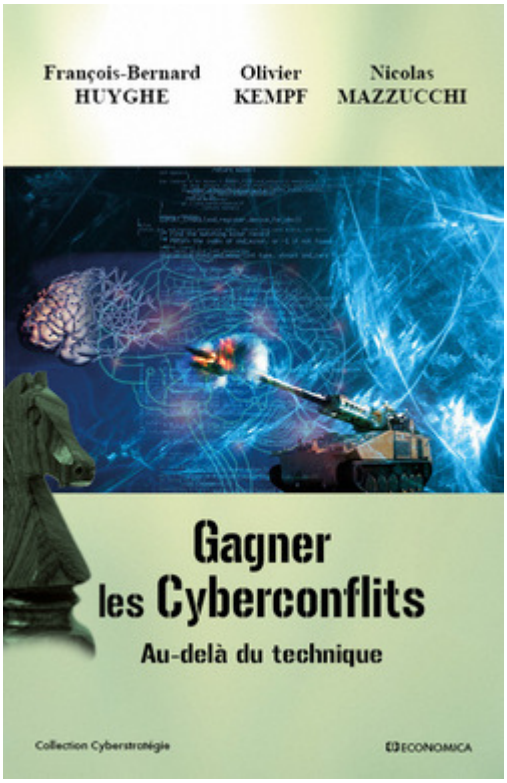
Ensuite, la robotique se rapproche beaucoup de l'Internet des objets. Elle a donc clairement à voir avec le cyberespace, c'est un saut dans la technologie de la guerre.

De plus, un thème très populaire depuis un an environ est l'intelligence artificielle, c'est-à-dire l'autonomisation des systèmes. Cela se développe quelque part dans la fusion entre le *cloud* et le *Big Data* d'un côté, et la robotisation de l'autre.

Enfin, il y a la fusion entre le cyber et l'humain. Cela peut être un vrai choc et il ne sera pas forcément technologique. Comme on l'a dit tout à l'heure en abordant le critère de létalité, aujourd'hui une cyberattaque ne tue pas un humain. Le jour où des outils cyber seront greffés à l'humain, cette frontière de létalité risque peut-être de se déplacer. Je parle bien sûr de potentialité, je ne suis pas dans la prévision. Derrière les fantasmes hollywoodiens de l'homme bionique, il y a aujourd'hui une possibilité prospective à envisager : nous ne sommes donc pas dans la prévision mais il est clair que nous ne sommes plus dans la fiction.

Plus

. François-Bernard Huyghe, Olivier Kempf et Nicolas Mazzucchi de *Gagner les cyberconflits. Au delà du technique* , Paris, éd. Economica.



4e de couverture

Le cyberespace couvre trois couches : physique (les matériels), logique (les logiciels) et sémantique (l'information qui circule dans le cyberespace). Les études sur la cyberconflictualité se concentrent le pus souvent sur la couche logique. Or, la couche sémantique, absolument déterminante, constitue l'objectif final de bien des cyberagressions.

Malgré les points communs, on ne peut réduire l'action dans la couche sémantique à la guerre de l'information ou à la communication stratégique : une cyberstratégie se dirige en premier lieu contre l'adversaire, même si cette action peut passer aussi par le public. Elle n'est pas non plus une simple subversion : la majorité des cyberagressions (le livre est fondé sur l'analyse d'une quarantaine de cas) combine des actions dans les trois couches et sont composites (espionnage, sabotage et subversion).

Gagner le cyberconflit suppose bien sûr des calculs et des computations dans la couche logique. Mais il n'est pas un virus, pas un ver, pas un maliciel, aussi évolué soit-il, qui n'atteigne son but si la dimension sémantique a été omise du calcul stratégique.

François-Bernard Huyghe, Olivier Kempf et Nicolas Mazzucchi sont chercheurs à l'Institut des Relations Internationales et Stratégiques (IRIS), spécialisés en cyberstratégie et en géoéconomie. Ils ont écrit ce livre à l'issue d'une étude effectuée au profit du Conseil Supérieur de la Formation et de la Recherche Stratégiques (CSFRS).

Voir le livre de François-Bernard Huyghe, Olivier Kempf et Nicolas Mazzucchi de *Gagner les cyberconflits. Au delà du technique* sur le site des éditions Economica

---

P.-S.

François-Bernard Huyghe est Docteur d'Etat en sciences politiques et habilité à diriger des recherches en sciences de l'information et de la communication. Olivier Kempf est Docteur en Science politique, Chercheur associé à l'IRIS. Ils sont co-auteurs avec Nicolas Mazzucchi de « Gagner les cyberconflits », Paris, éd. Economica. Propos recueillis par Yann Derriennic et Maxime Arquillière étudiants en Master 2 à l'Institut Français de Géopolitique. Avec l'aide de Léopold Jacqueline, stagiaire à la Chaire Castex de Cyberstratégie.

Notes

[1] Jean Guisnel, un des plus réputés journalistes de défense, révèle dans Le Télégramme de Brest l'opération d'espionnage, sans en désigner l'auteur, même s'il suggère non des Chinois, mais des « alliés » (sans autre précision).