Une cyberstratégie à inventer

Monsieur François-Bernard Huyghe
Docteur d'État en Sciences Politiques
Chercheur à l'Institut des relations internationales et stratégiques

S'il est un domaine où notre pays n'est pas absent, au moins en termes de réflexion théorique, ou d'intentions politiques, c'est la cyberstratégie[1]. En attendant peut-être que la France se dote d'une « quatrième armée », après l'air, la mer et la terre, pour lutter dans le champ de bataille numérique, nous sommes tous bien conscients de la nécessité d'un art de vaincre adapté à ce milieu. Mais comment peut-on gagner « dans » le cyberespace ? Là où la guerre ne consiste plus à porter son territoire derrière la frontière de l'autre, où il n'y a pas de capitales ennemies à occuper ni de cibles à bombarder et où ne servent guère les gros bataillons[2].

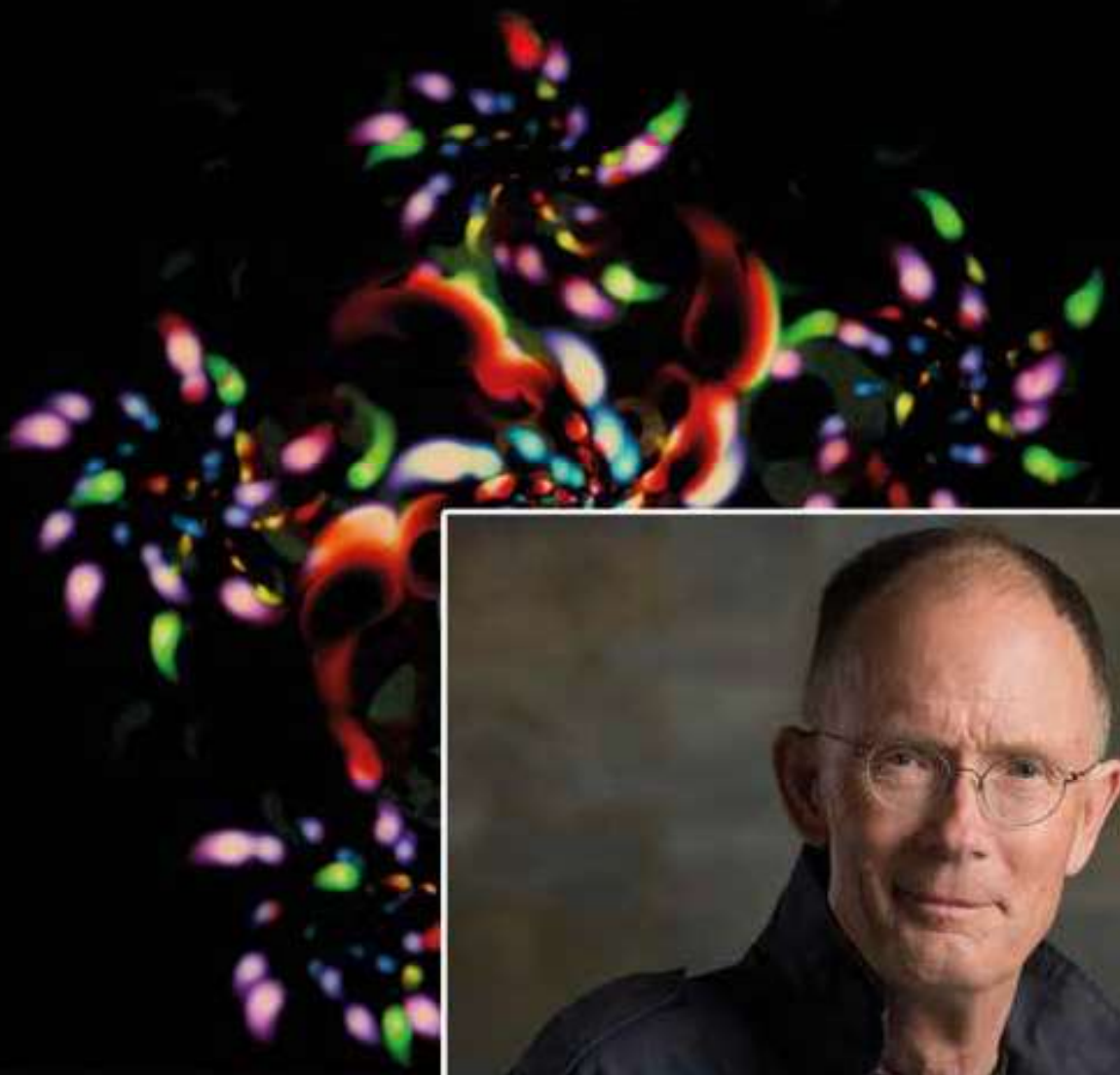
L'origine du terme cyberespace est un livre de science fiction de 1984, (le *Neuromancien* de William Gibson). Il est forgé à partir de « cybernétique » (initialement science du « gouvernail » ou des automates) plus « espace ». Il renvoie à « *une représentation graphique de données extraites des mémoires de tous les ordinateurs du système humain* ». L'expression, vite popularisée, s'est imposée pour désigner le « monde » né de la connexion des ordinateurs échangeant des données et de tout ce qui les fait fonctionner, matériel ou immatériel.

Cette interface au croisement du numérique (qui réduit toute information à une série de bits reproductibles, transportables, combinables comme à l'infini) et des réseaux qui en assurent la circulation parle à l'imagination : un monde derrière les écrans, comme le pays des merveilles d'Alice est de l'autre côté du miroir.

1. On songe à la place de la cyberstratégie dans les Livres blancs depuis 2008, au « pacte cyber » de 2014, à l'existence de deux chaires de cyberstratégie en France, à l'abondance des publications...
2. Nous tenterons de répondre à cette question dans *Gagner le cyberconflit*... co-écrit avec N. Mazzucchi et O. Kempf, et à paraître prochainement aux éditions Economica.

MODERN MASTERWORK

w1ll1am g1bs0n



neuromancer

Pour qu'un tel monde existe, il faut trois composantes :

- des « choses », des écrans, des câbles, des antennes..., soumis quelque part au pouvoir d'une autorité ;

- des « codes », applications, algorithmes, protocoles..., ce qui veut dire qu'en ce domaine des innovations et informations nouvelles, par exemple sous forme d'un algorithme inédit comme un maliciel, peuvent très rapidement bouleverser des rapports de force ;

- des « signes » qui ont du sens pour un destinataire, un cerveau humain, donc avec une part d'imprévisibilité et de subjectivité qui touche la nature et l'ampleur des effets obtenus (désordre, peur, agressivité, mobilisation...).

Il est donc convenu, pour les désigner de parler de couche matérielle, logicielle et sémantique du cyberespace.

Les choses sont quelque part (par exemple un câble sous-marin formant une dorsale d'Internet passe dans telles eaux territoriales où il est possible d'y prélever des flux d'informations). Les codes ont été fabriqués par quelqu'un (qui a pu, par exemple, installer une « porte de derrière ») et ils peuvent subir l'action d'autres codes (tel un système de contrôle informatique type SCADA qui peut être déréglé par un logiciel malveillant). Quant aux signes, ils s'adressent à des gens chez qui ils suscitent des réactions : ils savent ou croient des choses, et sont amenés à prendre des décisions, en fonction de ce que leur montrent leurs ordinateurs et de leur interprétation. Maîtriser des infrastructures de communication, inventer des algorithmes redoutables et agir sur autrui par écran interposé : déjà se dessinent des pistes.

Le cerveau humain, cible ultime

La cyberstratégie, par essence humaine, s'applique à un espace technique, produit artificiellement, et sa finalité reste dans le monde réel : obtenir quelque chose de quelqu'un par la force et la ruse.

Au final, la cible ultime reste bien ce cerveau humain. En stratégie classique, la violence vise à agir sur la volonté de l'ennemi, soit, radicalement, en le tuant, soit en l'amenant à se rendre, à poser les armes, à accepter vos condi-

tions de paix, etc. Dans le cyberespace, par des moyens informatiques, il est possible d'agir sur un adversaire (ou une victime) en diminuant des capacités (en lui volant des connaissances précieuses, en empêchant ses outils de décision et de coordination de fonctionner), en le trompant ou en l'influençant.

Pour ce faire, le numérique offre des possibilités inédites de pénétrer dans un système adverse pour y voler des données confidentielles (espionnage) et aussi pour empêcher ledit système de fonctionner correctement (sabotage). Ce dernier point vaut qu'il s'agisse de paralyser une chaîne d'enrichissement de l'uranium iranienne (opérations dite Stuxnet menée en 2012) ou une chaîne de télévision francophone (TV5 condamnée à l'écran noir au mois d'avril 2015). Enfin, il est possible de mener une action psychologique ou symbolique (que certains nomment « de subversion ») contre des organisations ou des communautés cibles. Dans des genres très différents les *Anonymous* qui peuvent « *défacer* » ou submergent de demandes (*Divided Denial Of Access*) des sites d'organisations adverses le font toute la journée, mais aussi les pirates informatique pro Bachar El Assad de la *Syrian Electronic Army*.

Ajoutons un dernier élément : l'imaginaire. Dès les années 90, Internet avait suscité les prédictions les plus triomphales : « toutes » les informations possibles seraient disponibles et tous pourraient communiquer avec tous ; toutes les frontières et les délais seraient abolis, nos systèmes politiques, économiques et culturels en seraient révolutionnés, etc. Mais il a aussi nourri toutes les craintes : les « *cavaliers de l'infocalypse* » (pédophiles, nazis, terroristes, trafiquants en tout genre) allaient y proliférer, mais surtout des attaques destinées à piller, à créer du chaos ou à manipuler les foules menaceraient nos biens, nos institutions et nos valeurs. Demain la cyberguerre (notion fort douteuse) allait bouleverser l'équilibre international, des actions « cyberterroristes » permettaient à une poignée d'hommes de mettre à genoux nos sociétés ouvertes de l'information, si dépendantes, justement, de leurs systèmes d'information. Outre-Atlantique, se poursuit l'attente du « Pearl Harbour informatique » (ou du Cybergeddon, cyber + Armageddon, la fin du monde) – comprenez la peur d'une attaque contre les systèmes informationnels d'un pays qui paralyserait une fonction vitale comme l'approvisionnement énergétique.

Pour le moment, personne n'est mort d'une cyberattaque, aucun pays n'a dû se soumettre à un autre sous la contrainte d'un virus informatique particulièrement puissant et les terroristes préfèrent globalement utiliser des Kalachnikov plutôt que des McIntosh.

Mais en même temps, il semble évident qu'il y aura une composante cyber dans la plupart des conflits. Ceci vaut qu'il s'agisse d'affrontements militaires classiques (quel belligérant se priverait d'essayer de pénétrer de paralyser les systèmes adverses avec un algorithme plutôt qu'avec un commando ou un missile ?) ou de conflits idéologiques (quelle guerre des idées ne se prolonge pas sur les réseaux sociaux ?). Et, bien sûr, dans un système comme le nôtre dépendant de plus en plus de la circulation de l'information numérisée, les enjeux économiques sont énormes.

Vulnérabilités et conflits

Le cyberespace permet de plus en plus d'agir dans les secteurs, géopolitiques militaires, idéologiques ou économiques comme l'ont compris les acteurs qui l'utilisent, souvent en dissimulant leur identité. Parallèlement, l'abolition de la barrière entre producteurs et consommateurs d'informations dans les réseaux sociaux et le Seb 2.0 facilite l'entrée sur le champ de bataille et fait encore davantage de l'information à la fois un enjeu et une arme, un objectif et un bouclier. Plus une société devient « de l'information », plus elle est dépendante de données, de systèmes, de réseaux et de dispositifs lointains par définition vulnérables. Plus il est tentant de se livrer à la prédation ou à la perturbation par électrons interposés.

D'où une tendance lourde. Si des cas de cyberattaques ont été signalés dans les années 1990, à partir de la seconde moitié des années 2000 naît vraiment l'univers conflictuel voire chaotique que nous connaissons.

Aujourd'hui lire dans la presse (comme c'est le cas le jour où nous écrivons ces lignes) « *cyberattaque préoccupante contre la Maison Blanche* » relève de la routine : nous avons parfaitement intégré qu'il n'y a plus guère de grande organisation ou institution qui ne constitue une cible, et que l'on peut voir son système informatique pénétré à distance (pour vous voler des donner précieuses, mais peut-être aussi vous humilier, vous défier, vous lancer un avertissement), qu'il faudra s'adapter et que cela se reproduira sans doute plus tard, sans que cela implique la guerre finale ou le chaos total.

Tous les grands types d'acteurs, États, organisations, groupes activistes et individus, ont investi le cyberespace avec une énergie et avec une inventivité croissantes. Au prix d'une complexité préoccupante. À commencer par la difficulté qu'il y a à déterminer l'identité et le but véritable des acteurs,

protégés par le brouillard qui entoure toute attaque : d'où venait-elle (pas forcément de celui qui la revendique) et que visait elle qu'elle ait réellement atteint ? La chose est bien moins claire que lorsque des tanks violent une frontière.

Bref, si la nécessité d'une cyberstratégie s'impose dans tous les pays, elle soulève partout les mêmes questions – Comment protéger ses infrastructures vitales ? Comment faire coopérer acteurs privés ou publics ? Faut-il se doter d'armes informatiques offensives ? Que faut-il avouer ou laisser croire en ce domaine ? Jusqu'où aller dans la protection de sa souveraineté numérique et dans le respect de celle des autres ? Comment se reposer sur le droit ou sur ses alliés ? À partir de qu'elle nocivité de l'attaque se considérer comme victime d'un acte de guerre ? Quid du facteur temps (temps de préparation, décèlement, résilience) ? Tous y apportent des réponses qui reflètent à la fois leurs intérêts et leurs cultures stratégiques.

Pour ne donner qu'un exemple, le Département de la Défense américain qui classe la cyber menace au sommet des dangers à combattre vient de publier sa nouvelle cyberstratégie[3]. Il se donne pour objectifs la défense de ses propres réseaux et des intérêts vitaux du pays face à des attaques de perturbation, mais aussi la maîtrise de ses propres armes informatiques pour mener des opérations (qu'il faut bien parfois présumer offensives) dans le Cyberespace. Significativement aussi, il considère son usage comme susceptible d'aider à contrôler l'escalade des conflits et de s'intégrer dans toutes les options militaires. Sans oublier la question des alliances dans le cyber.

Visiblement, la dimension cyber sera désormais partout dans le conflit, non pas sous forme d'une hypothétique cyberguerre qui remplacerait la guerre tout court, mais comme une vulnérabilité obsession, un moyen d'attaque et de défense y compris civile, une composante à intégrer à des modes de lutte plus classiques, mais aussi une option nouvelle ouverte au politique pour envoyer un message (pression, avertissement, menace, punition...) et agir sur la volonté politique de l'autre.

3. *The DOD Cyberstrategy*, avril 2015, http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Puissance technologique et anticipation psychologique

En croisant les grilles que nous venons de présenter, il commence à s'esquisser quelques tendances d'une future cyberstratégie. Elle suppose une démarche, d'ailleurs bien entamée en France, et qui ne se borne pas à dresser des défenses de plus en plus solides contre des attaques de plus en plus imprévisibles. Elle demande de la continuité politique et une vision à long terme.

Il faudra bien sûr de l'excellence technique, toujours plus de coopération entre secteurs privé et public, de la sensibilisation des acteurs, de l'anticipation (y compris dans le choix des matériels, des logiciels, du stockage de données « dans les nuages », qui répondent à des critères nationaux ou au moins européens de sécurité), toujours plus de réactivité.

Il faudra aussi davantage de renseignement, ne serait-ce que pour déceler qui pourrait vouloir s'en prendre à nous par écran interposé et dans quel but. Il faudra certainement aussi intégrer un élément psychologique, de la crédibilité : une attitude (une posture, diront les militaires) qui décourage de futures agressions, moins par l'étalage de moyens informatiques (affaiblis aussitôt que révélés, sans doute éphémères face à la prochaine innovation agressive), que par la crainte qu'un pays de notre niveau technologique, ayant la volonté de se défendre, ne puisse exercer une rétorsion, même contre ceux qui se croient à l'abri derrière des écrans lointains.

Enfin et surtout, nous aurons besoin de réinventer des règles pour nous adapter à un monde de l'innovation technique et du changement stratégique. Le défi n'est pas seulement lancé à nos capacités scientifiques mais aussi à notre souplesse mentale. Avantage au rapide et à l'inventif. Est-ce une nouvelle qu'il faille redouter ?