Offensif et Défensif

François Bernard Huyghes, Directeur de Recherche, IRIS

Mai 2013, Article n°III.4

Traditionnellement, est considéré comme arme "offensive" tout artefact qui sert à infliger une perte humaine ou matérielle[1]. Est donc logiquement réputée défensive une arme (ou un système de protection) visant à rendre inutile la première. Dans la réalité les deux se combinent et l'on porte une épée et un bouclier, un tank a un blindage et un canon, etc.

Stratégiquement parlant, l'offensive a longtemps consisté à lancer des hommes, des véhicules, des forces ou des projectiles contre l'Autre, l'action défensive étant forcément seconde et réactive. D'où la logique des indices utilisés pour juger qui attaque et qui se défend : l'initiative, la violence et le lieu de la première attaque.

Il y plus d'un siècle, Ratzel[2] pouvait dire que la guerre "consiste à porter sa frontière sur le territoire de l'autre". Comprenez : accomplir des actes de domination ou de violence au-delà de la frontière politique, frontière dont l'étymologie est précisément "ligne de front" : confronte la ligne adverse et marque provisoirement la zone au-delà de laquelle la bataille est possible, mais en deçà de laquelle un camp est à l'abri[3]. Notion que la cyberattaque, en dissimulant son lieu d'origine, rend douteuse

Tout ceci ne va pas forcément sans ambiguïtés. Un exemple extrême est celui de la guerre "préemptive" (et non préventive) imaginée par G.W. Bush[4] et ses conseillers néoconservateurs : cette doctrine autorise à frapper un ennemi (État-voyou ou groupe terroriste abrité par un État) qui se préparer à attaquer de façon imminente, surtout s'il est doté d'armes de destruction massive ou sur le point d'en acquérir. Tout en se disant en légitime défense.

Information ravage et information bouclier

[1] André Leroi-Gourhan (*Évolution et technique*, 2 vol. T II *Milieux et techniques*, 1943, Albin Michel) expose une logique de l'évolution de l'arme.
[2] Friedrich Ratzel, *Géographie politique*, 1897, édition française : 1988, Economica
[3] Sur l'évolution et les ambiguïtés de la notion de frontière, voir Médium n° 24/25 *Frontières*, 2009, Ad Rem
[4] Discours de West Point du 1° juin 2002, voir notre commentaire dans F.B. Huyghe, *Quatrième guerre mondiale Faire mourir et faire croire*, 2004, Éditions du Rocher

Comment transposer ces notions dans le monde cyber ? Les termes que l'on rencontre désormais - lutte informatique offensive (LIO[5]) et de la lutte informatique défensive (LID) - présupposent qu'une attaque informatique puisse faire ravage par électrons interposés.
Cette opération ne consiste plus à projeter des gens, des choses ou de l'énergie vers un territoire, mais à introduire une information - programme malveillant ou message déstabilisateur - dans un dispositif adverse. Le dommage que subit la victime est une perte - de son patrimoine informationnel, de sa capacité de contrôle ou de son image.[6]

Ceci renvoie à une redéfinition de l'arme. L'attaque cyber ne peut, dans une première phase au moins, que dérober ou deviner par ruse ou par technique une information que "possède" la victime ou un tiers (un ordinateur-zombie dont l'agresseur prend le contrôle pour mener une attaque par déni d'accès partagé, p.e.). Dans le vocabulaire de la cybersécurité, il est question de la confidentialité, de l'authenticité, de la fiabilité ou de l'intégrité de l'information[7]. En d'autres termes l'attaquant commence forcément par s'en prendre à un bien intellectuel (sous forme de signes stockés dans des machines) et en altère les propriétés, ce qui semble à cent lieues de la brutalité qu'évoque habituellement une attaque : frapper, tirer, etc.

Toute attaque informatique suppose une résistance sémantique et technique surpassée (et un secret dérobé[8]) : que l'on ait volé un mot de passe, franchi une "barrière de feu" (*firewall*), craqué un système de détection, bref que l'on se soit introduit "dans" un espace protégé (le disque dur d'un ordinateur, un téléphone, un système d'information...) tout se fait par signes interposés. Et ceci par intrusion, contre une défense trop faible (si les contrôles de sécurité étaient parfait et les hommes assez méfiants, la question de l'attaque ne se poserait même pas). De la première "violence" que constitue l'intrusion en naît une seconde qui consiste en trois choses, ou une combinaison des trois via des instructions illégitimes à un cerveau électronique:

- prendre connaissance d'informations confidentielles, i.e. espionner

- détraquer un système (il ne contrôle plus, il n'avertit plus d'une anomalie, il ne fonctionne plus...), ce qui revient à saboter

- y laisser une trace (un tag vengeur, un slogan, une information fausse...) équivalent de défier ou désinformer[9].

À un troisième stade, l'attaque peut produire un dommage indirect dans le monde physique. Par exemple un système SCADA[10] de contrôle industriel se détraque et une usine ne fonctionne plus, ou une organisation se trouve incapable de communiquer normalement donc livrée au chaos ou encore un système radar ne décèle pas une attaque, un hôpital est privé d'électricité et quelqu'un meurt...

---

[5] Magazine MISC n° 36 *Lutte informatique offensive*, 2008, éditions Diamond, notamment l'article d'Éric Filiol
[6] Sur la notion de ravage et violence par l'information voir Françoi-Bernard Huyghe, *L'ennemi à l'ère numérique*, P.U.F., 2001
[7] Voir par exemple la norme ISO 2700 (Système de management de la sécurité de l'information)
[8] Edith et François-Bernard Huyghe, *Histoire des secrets*, 2000, Hazan, p.227 et sq.
[9] Sur la notion de désinformation, voir : revue Panoramiques N° 58, *Désinformation, tous coupables ?*, 2002 et *La désinformation, pour une approche historique*, Colloque de Montpellier du 18 et 19 11 1999, Université Paul Valéry, 2001
[10] SCADA : Supervisory Control and Data Acquisition

Le second stade (celui des instructions illégitimes) la perte subie est souvent celle d'un monopole (p.e. un rival économique s'empare de données protégées ce qui lui donne un avantage concurrentiel illégitime) ou une perte de prestige (l'adversaire a prouvé qu'il pénétrait sur votre site quand il voulait et réalisé un exploit). Variante : l'attaque crée une illusion : vous croyez vous adresser à X et vous êtes en contact avec Y, vous croyez que Z a dit blanc, et il a dit noir... Mais ces opérations intellectuelles ne produisent encore ni cadavres sanglants, ni ruines fumantes, avant qu'advienne le dommage, direct ou indirect : les données ou la confiance perdues, l'argent qui s'est évaporé, le désordre qui s'est créé, voire les dégâts physiques ou humains en bout de chaîne.

Le problème est ici de déterminer quel degré de nuisance (à chacun des stades) est assez grave pour déclencher une procédure de crise, une réaction vigoureuse, un réexamen de tout votre système de protection, voire une guerre (puisque des cyberattaques[11] peuvent être considérées comme des actes de guerre, notamment par les États-Unis).[12]

Purement défensif ?

On se doute que la cyberdéfense comprend tous les moyens d'empêcher ce qui précède ou de gagner une résilience rapide en cas d'attaque. Des moyens physiques et virtuels qui vont de l'anticipation ou de la détection des attaques à la construction de défenses plus solides (meilleurs antivirus, meilleure cryptologie, meilleurs systèmes de Firewall, résilience fiable, sensibilisation des acteurs, mise sur pieds d'équipe de diagnostic et d'intervention rapides et efficaces, partage de l'information sur les attaques subies, précaution et prévention par des outils techniques et des comportements vertueux, coopération, etc.) bref à peu près tout ce qu'encourage l'ANSSI[13] en France et dont il faut se féliciter.

Tous les pays qui reconnaissent posséder des armes offensives sont discrets à leur sujet : dire quel arme on prépare, quel type de virus ou quel type de "zero day attack" (attaque qui exploite une faille jusque-là jamais publiée, constituant ainsi une sorte d'exploit inédit) on envisage, c'est révéler ce que l'on peut faire et contre qui on compte le faire, donc doublement avertir l'adversaire présumé qu'il est visé et comment. Cela peu lui donner tout le temps nécessaire pour réparer sa vulnérabilité.

L'arme offensive, dont on peut présumer que, si elle est utilisée effectivement, elle incitera à réparer les failles, risque peut-être de ne servir qu'une fois. D'où l'avantage, que souligne le Sénateur Bockel,[14] de ne pas décrire trop précisément son arsenal : l'incertitude d'un éventuel agresseur ne peut que contribuer à le faire hésiter (ou choisir des cibles plus "molles"). À défaut d'un effet de dissuasion[15] on peut espérer un peu de précaution chez l'autre.

Restera à expliquer comment on peut être purement défensif sans être quelque peu offensif : la défense la plus efficace ne reposerait-elle pas sur la connaissance des mécanismes adverses (donc sur "un petit peu" d'espionnage ou de piraterie) ? N'est-il pas tentant de tendre des pièges à des candidats à l'agression ? Comment résoudre la question de l'attribution sans

[11] Daniel Ventre, *Cyberattaque et cyberdéfense*, Lavoisier, 2011
[12] New York Times, 31 Mai 2011, *Pentagon to consider Cyberattacks as Acts of War*
[13] Agence Nationale pour la Sécurité des Systèmes d'Information
[14] Rapport d'information de M. Jean-Marie Bockel, commission des affaires étrangères, de la défense et des forces armées, n° 681, 18 juillet 2012
[15] Voir B. Gruselle, B. Tertrais et A. Estarl, *Cyber Dissuasion*, Recherche et Documents, Mars 2012, ainsi que Martin Libicki, *Cyberdeterrence and Cyberwar*, Rand 2009

devenir pro actif ? Comprenez : sans violer à son tour les secrets de l'autre, le piéger et l'égarer?

Enfin quid du "préemptif" ? Lancer une attaque "juste à temps" contre un État qui s'apprête à vous agresser ne suppose-t-il que l'on ait soi-même pénétré les secrets de sa défense ? Si les rumeurs qui annoncent que l'administration Obama envisage une action cyber préemptive se confirment[16], ce pourrait être un singulier effet d'abyme où il deviendrait de plus en plus difficile de différencier l'agresseur du défenseur. Et ce à mesure que s'accumuleront les différends[17] (accusation d'espionnage, par exemple) source de tout conflit.

Les deux caractères présumés de l'arme défensive - être techniquement différente de l'arme offensive, ne servir qu'en réponse à une attaque préalable - deviendront sans doute plus problématiques à mesure que se développeront les cyberstratégies. D'une part parce que, dans le cybermonde, "connaître" son adversaire peut difficilement se faire sans s'emparer informations qu'il dissimule et, d'autre part, parce que les jeux de la dissimulation et de rhétorique auxquelles les cyberpuissances seront amenées à recourir feront aussi de l'arme - réelle ou virtuelle - des objets de menace, de dénonciation et de négociation, donc des valeurs symboliques d'échange.

Fondation Saint-Cyr, Ecole militaire, 1 place Joffre, 75007 Paris
Téléphone: 01-45-55-43-56 - courriel: contact@chaire-cyber.fr; SIRET N° 497 802 645 000 18

La chaire remercie ses partenaires

[16] David Sanger et Thom Shanker, *Broad Powers for Obama in Cyberstrikes*, New York Times, 03 Février 2013
[17] Jean-François Lyotard, *Le différend*, Éditions de Minuit, 1983