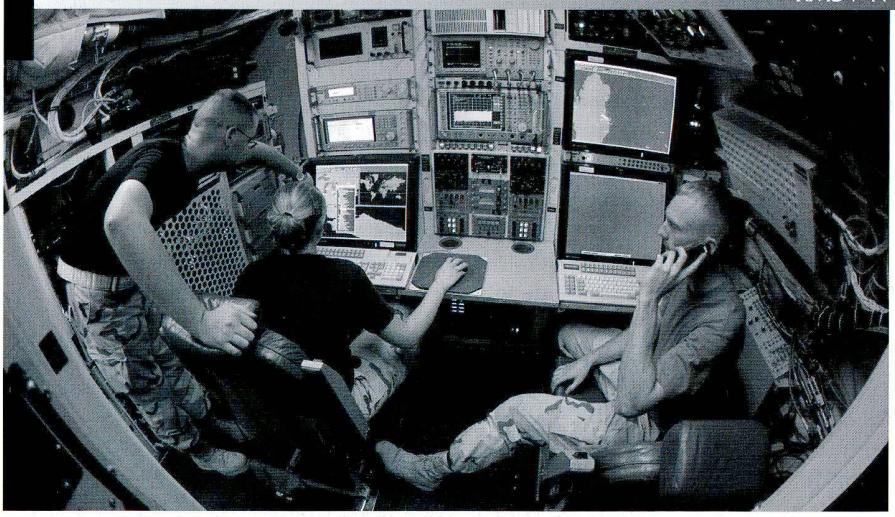
Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2008)
Heft: 5

Artikel: Un cyberconflit est-il possible?
Autor: Ventre, Daniel
DOI: https://doi.org/10.5169/seals-346911



Des appareils de mesures et d'écoute électroniques, tels l'EC-135 américain, volent dans l'espace aérien international et identifient les signaux électromagnétiques, en temps de paix déjà. Leur apport est primordial pour la préparation d'une opération militaire de grande ampleur. Photo : US Air Force.

Un cyberconflit est-il possible ?

Daniel Ventre

CNRS - chercheur au CESDIP *

A l'heure de la modernisation des armées (RMA) contrainte par la révolution des technologies de l'information et de la communication, au moment où les militaires s'interrogent ou s'engagent dans la reformulation de leurs doctrines militaires pour les confronter aux nouvelles réalités d'un monde globalisé, les grandes nations sont lancées dans une course au réarmement, les équilibres mondiaux sont en pleine reconfiguration et se dessinent les nouveaux contours de l'ordre planétaire de ce début de XXIe siècle. L'état de paix dans lequel nous vivons peut paraître bien fragile, même si les soixante années passées nous avaient habitués à regarder la guerre se dérouler loin de chez nous.

Après que nos sociétés civiles aient été accoutumées au discours sur la guerre économique, présentée comme le substitut aux conflits armés, comme la forme ultime de l'affrontement moderne entre les nations, elles ont fini par en oublier la probabilité et la possibilité du retour, dans nos murs, à des formes de conflits plus violents, plus destructeurs : les conflits armés. La menace s'est introduite avec violence le 11 septembre 2001 dans la forteresse abritant notre civilisation. Le terrorisme s'est invité sur la scène des affrontements entre les puissances. Et dans notre univers désormais réseau-centré, la menace prend une nouvelle forme, celle de l'agresseur invisible, indécelable, qui en deux clics de souris ou presque pourrait faire vaciller le fonctionnement d'un Etat, paralyser ses infrastructures sensibles, voire ses armées. Les vagues de cyber-attaques subies ces dernières années (par exemple les affaires *Moonlight Maze* et *Titan Rain* aux Etats-Unis entre 1999 et 2003) et ces derniers mois (Estonie en avril 2007, Etats-Unis en juin et octobre 2007, Allemagne et France en août 2007, Grande-Bretagne en novembre de la même année), touchant les Etats au cœur de leurs systèmes sensibles, et généralement mises sur le compte des gouvernements russes et chinois, nous font-elles prendre la vraie mesure des menaces qui planent sur nos sociétés devenues totalement dépendantes de leurs systèmes d'information ? Ces « attaques » sont peut-être un avant-goût des nouvelles formes d'affrontements entre les peuples. Un cyberconflit est-il alors possible ? La réponse n'aura rien d'affirmatif ni définitif. Elle ne pourra au contraire qu'en appeler bien d'autres.

Qu'est-ce qu'un cyberconflit ?

Avant même d'envisager la possibilité d'un tel conflit, il convient de le définir. Le conflit est une lutte, un combat, une rencontre provoquant une opposition. Pour les militaires, le conflit est guerre, lutte armée entre groupes sociaux. Le terme « cyberconflit » peut quant à lui recouper bien des formes diverses du conflit.

Il peut en effet désigner la forme que prend le conflit : Les affrontements idéologiques, politiques, de valeurs, qui opposent les « hacktivistes » dans le cyberespace, et qui expriment leurs revendications au travers de défigurations de sites ou d'attaques DoS.
Les *Computer Network Attacks* (CNA), c'est-à-dire les attaques menées sur les réseaux (attaques virales, DoS, intrusions, etc.), contre les systèmes d'information de pays étrangers, en temps de conflit mais également en temps de crise ou de paix. Les opérations peuvent être menées indistinctement par les militaires ou les civils, de manière agressive, défensive, préemptive, etc. Les évènements de 2007 évoqués plus haut sont une manifestation de ces CNA. Mais il s'agira alors d'être en mesure de faire la distinction entre les actions de cybercriminalité (relevant du droit pénal des Etats, de la coopération judiciaire) et les opérations qui véritablement sont affrontement, conflit (lesquelles relèveront alors du droit international, du *Jus ad Bellum, Jus in Bello*, Charte des Nations Unies, Conseil de Sécurité, OTAN, etc.). Seulement dans le dernier cas pourra-t-on parler de cyberconflit.

* Centre national de la recherche scientifique (CNRS). Auteur de *La guerre de l'information* aux Editions Hermès Lavoisier.

Les actions agressives dans le cyberespace, qui prolongent des évènements survenus dans le monde tangible. Ainsi les vagues d'agressions contre les systèmes d'information estoniens n'ont-elle été que le prolongement dans le cyberespace des émeutes qui avaient enflammé les rues de la capitale pendant plusieurs jours, opposant communautés russes et estoniennes. Ce phénomène de prolongement dans le cyberespace des tensions, crises et conflits développés dans le monde tangible est observé régulièrement depuis plusieurs années.
Le cyberconflit a longtemps été associé à l'expression « Pearl Harbor informatique », désignant une attaque fatale, paralysante, décisive, brutale, imparable, imprévisible, contre les systèmes d'information d'un adversaire, qui n'aurait ni le temps de réagir, ni de se relever, s'organiser, permettant ainsi à l'agresseur de gagner en un seul coup, avant même de réellement combattre. Gagner avant d'avoir déclaré la guerre est une idée séduisante, que l'on prête encore à la doctrine militaire chinoise par exemple.

Le « cyberconflit » peut faire référence à la dimension dans laquelle se déroule le conflit :
Le cyberconflit désignerait alors toute forme conflictuelle se déroulant au sein de l'espace informationnel. Mais pour autant, un conflit pourrait-il s'exprimer uniquement au sein de cet espace ? Un conflit qui se manifestera dans le cyberespace y trouvera plus probablement une voie nouvelle, complémentaire, mais qui ne se substituera pas à ses dimensions plus traditionnelles que sont la terre, l'air, la mer et l'espace. Et ce d'autant que l'espace informationnel est davantage un espace transversal, commun aux autres dimensions du conflit, qu'un espace isolé, coupé du monde, capable d'imposer seul son verdict au conflit tout entier. Les grandes armées du monde ont déjà intégré cette dimension informationnelle et en ont fait leur espace de combat, notamment en implémentant les systèmes C4ISR, ou encore dans la formulation de leurs doctrines au travers du concept de « guerre de l'information. » La maîtrise de cet espace informationnel est l'un des objectifs majeurs de la RMA.
Des acteurs non militaires s'invitent dans ces conflits de nouvelle génération et le conflit mené dans le cyberespace autorise la participation de civils, de troupes armées régulières, de combattants d'armées non régulières, de s'affronter, de faire la guerre. Ces acteurs non militaires sont-ils en mesure de perdre/gagner un conflit en lieu et place des militaires ? Le cyberconflit pourrait-il être un conflit strictement non militaire ?

Le « cyberconflit » peut faire référence à l'arme qu'utilise le conflit :
L'arme est ici la technologie qui donne son nom à la guerre. L'arme est le cybernétique. La guerre est celle de l'information. Cette forme de guerre est contemporaine de la guerre chimique, de la guerre bactériologique, de la guerre nucléaire, de toutes ces technologies létales qui donnent leur nom à une forme de conflit spécifique.
L'espace informationnel est utilisé comme arme pour dominer, maîtriser un adversaire. Les Etats-Unis ont pour objectif la « dominance de l'information ». Grâce à la maîtrise de cet espace, la victoire doit être sinon assurée, du moins facilitée. L'enlisement du conflit en Irak démontre que la dominance de l'espace informationnel n'est pas la seule condition garante du succès. Les capacités de guerre asymétrique, y compris dans le cyberespace, démontrent également que la dominance absolue – pour autant que cette mesure soit proportionnelle à la débauche de moyens technologiques mis en œuvre – n'est pas une certitude de victoire.

L'armée canadienne dispose de 15 *Bison* 8x8 destinés à la conduite de la guerre électronique (CGE). Certains ont été déployés en Afghanistan.

Quel sens donner à « possible » ?

Un conflit possible est-il un conflit « probable » ? En ce cas, le cyberconflit, pour autant que les moyens soient réunis, est tout aussi probable qu'un conflit quel qu'il soit, car l'humanité semble avoir inscrit dans ses gênes le besoin d'affrontement, besoin que la révolution technologique n'a pas su mettre en sommeil.

Mais alors pourquoi un conflit qui pourrait se manifester dans d'autres espaces choisirait-il celui de l'information pour sa réalisation ? Quels sont les éléments déclencheurs du cyberconflit ?

Un ensemble de conditions nous paraissent devoir être réunies pour qu'un conflit éclate dans le cyberespace :

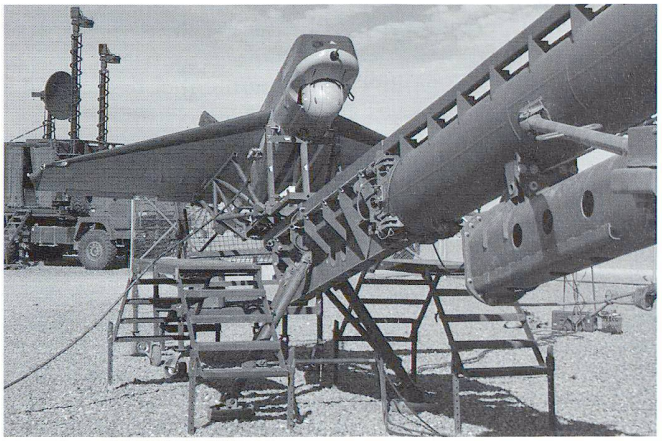
- Il faut qu'il y ait au moins deux acteurs en présence, belligérants. Une attaque unilatérale n'est pas un conflit. Il faut que les acteurs disposent des mêmes moyens. On ne peut parler de cyberconflit, quand bien même les plus complexes C4ISR seraient engagés, si l'adversaire en est à l'âge de pierre. Car l'objectif de la guerre de l'information et des cyberconflits est bien d'user des TIC, les siennes et celles de l'adversaire, pour déstabiliser, affaiblir, paralyser, observer, modifier le comportement de l'adversaire, altérer son processus de décision, l'isoler, le couper du reste du monde, dominer son espace informationnel, afin de prendre l'avantage dans la boucle OODA,[1] voir au-delà de l'horizon, et gagner sans combattre, combattre sans contact.
- Il faut des acteurs opportunistes, c'est-à-dire qui sachent attendre et détecter, voire provoquer, les failles et faiblesses de l'adversaire, qui sachent tirer parti du flou qui est entretenu aujourd'hui en temps de paix, pour tester leurs capacités tout en leur donnant l'apparence d'actions cybercriminelles.
- Il faut des acteurs en mesure de, et ayant comme volonté première, de porter atteinte à la souveraineté des Etats.
- Il faut des acteurs qui considèrent leur espace informationnel comme étant un réel domaine de souveraineté, comme le sont les espaces terrestres, maritimes, aériens.
- Il faut que les cibles possèdent les moyens de leur propre destruction, c'est-à-dire qu'elles soient fortement ou totalement dépendantes de leurs systèmes d'information. Plus leur dépendance sera forte, plus leurs capacités d'action dans le cyberespace seront fortes, mais aussi plus elles seront à la merci d'une action pouvant leur en faire perdre la maîtrise, plus les opérations de type EBO seront percutantes. C'est ce paradoxe, reposer sa puissance sur une force qui est sa principale faiblesse, qui rend les conflits asymétriques possibles, mais rend impossible un cyberconflit contre un acteur démuni de ressources informationnelles.
- Il faut des objectifs matériels aux conflits dans l'espace virtuel : action dans l'intangible mais objectifs dans le tangible.
- Il faut des acteurs capables d'alterner les arènes d'affrontement, car il est probable qu'un conflit et sa conclusion ne reposeront pas sur le seul verdict du cyberconflit.
- Il faut aussi des acteurs capables d'affronter des adversaires qui gravitent autour de structures organisationnelles en réseaux, parfois sans leaders (*stigmergie*), qui ont la capacité de se mobiliser rapidement, d'attaquer et disparaître immédiatement (*swarming*), ou au contraire peuvent être des acteurs très isolés, ou indécelables, non identifiables, indétectables, non localisables dans l'espace physique et virtuel.
- Il faut encore des acteurs en mesure d'anticiper, de se protéger, mais aussi de mener des actions offensives, agressives, préemptives en temps de paix et de crise, sans qu'il y ait encore conflit.

1 Cycle Observer – Orienter – Décider – Agir (OODA).

Les questions en suspens

Si le cyberconflit est possible : comment y entrer et comment s'en sortir ? Comment s'en protéger ? Comment s'en relever ? Face aux menaces de cyberconflits, la défense reste-t-elle une responsabilité nationale ? L'OTAN peut-il jouer un rôle ? Le principe de défense collective qui est celui de l'OTAN peut-il apporter une réponse satisfaisante pour contrer les nouvelles menaces ? Le droit international (*Jus ad Bellum, Jus in Bello*) peut-il seulement prétendre encadrer ces formes de conflits ?

D.V.



Les drones et l'exploration électronique livrent rapidement de grandes quantités de données, à l'instar de ce drone *Sprewer* canadien en Afghanistan.

Mais rien ne remplace le renseignement humain.