“Cyber” en bataille !

Par le colonel Aymeric Bonnemaison

Andromaque : *La guerre de Troie n’aura pas lieu, Cassandre !*
Cassandre : *Je te tiens un pari, Andromaque*.

Depuis le premier cheval de Troie informatique, ce débat entre Andromaque et Cassandre s’est porté sur l’imminence d’une cyberguerre. Aujourd’hui, Cassandre semble avoir gagné son pari. Les titres des journaux sont explicites : “La cyberguerre est déclarée !”, “la cyberguerre a commencé”. De son côté, Andromaque se fait plus discrète mais rappelle que cette guerre-là fait couler plus d’encre que de sang ; la vraie guerre est brutale et tragique, elle n’est pas virtuelle et immatérielle…

Pourtant, le “cyber” est déjà de tous les conflits. Il est central dans les opérations d’influence, d’agitation et de propagande. Il permet des raids discrets dans la profondeur d’un dispositif stratégique. Il s’insère dans les guerres classiques. Si l’on y prête attention, il y a désormais des batailles cyber en pagaille ! Cette prise de conscience ne garantit pas la victoire, mais son déni augure assurément d’une future défaite.

Pour tracer à grands traits le vaste monde du cyberespace, il est courant d’utiliser une définition par couches. Il y a d’abord la couche physique, celle des infrastructures de télécommunications et du stockage des données. Il y a ensuite une couche logicielle, celle des codes et des programmes, qui favorise le fonctionnement intelligent des réseaux. Enfin, il y a la couche sémantique, celle du sens, du contenu. Les batailles cyber se livrent dans toutes ces couches, à des degrés divers.

Le cyber dans la bataille de l’information

Le cyber est devenu l’acteur majeur de la guerre de l’information. La bataille qui se livre dans sa couche sémantique permet la manipulation des esprits à des fins d’agitation populaire et de déstabilisation. Sur Internet, il est aisé de créer des rumeurs, d’exacerber des rancœurs et de tromper des perceptions et des analyses. Ces procédés de déception et de leurrage ne sont pas nouveaux mais ils s’épanouissent tout particulièrement dans le cyberespace. Ce dernier permet en effet de couvrir instantanément le monde entier et de démultiplier le nombre d’acteurs potentiels.

Le cycle provocation-radicalisation

Il existe de nombreux exemples de dessins (caricatures de Mahomet…), de messages, de vidéos (le Coran brulé par Terry Jones en 2010, par exemple) dont la diffusion a généré des manifestations, des meurtres, des attentats, des soulèvements qui ont eu de graves répercussions géopolitiques.

Publié in ***Res Militaris*** (http://resmilitaris.net), **hors-série** “**Cybersécurité**”, **juillet 2015**

Par exemple, l'extrait d'un long-métrage intitulé "L'innocence des musulmans", mis en ligne le 11 septembre 2012, a entrainé de violentes manifestations en Indonésie, en Égypte, en Syrie, en Tunisie, au Pakistan, au Bangladesh, en Afghanistan… Ce film amateur de conception médiocre, volontairement caricatural, produit aux USA plus d'un an auparavant, ne bénéficiait jusque-là d'aucun écho. La mise en ligne de cette version courte, doublée en arabe, sur des réseaux sociaux pour le onzième anniversaire des attentats contre le Pentagone et le World Trade Center n'est pas un hasard. La vidéo est opportunément retransmise par des organisations musulmanes à tendances salafiste et djihadiste. Par des réactions en cascade, elle entraîne finalement l'attaque du consulat américain de Benghazi en Lybie et cause la mort de 19 personnes dont un diplomate américain. À Kaboul, le 18 septembre 2012, l'attentat-suicide d'une femme, revendiqué par Hizb-e-Islami en réaction au film, provoque la mort de 12 personnes dont 9 employés étrangers d'une entreprise de courrier international. Dans sa couche sémantique, la cyberbataille a déjà des morts à son actif.[1]

Entre terreur et fascination

Conscient des enjeux de la communication par Internet, les djihadistes (*Al-Qaïda* puis *Daech*) s'appuient outrageusement sur cette caisse de résonnance médiatique. Leur démarche dépasse aujourd'hui la simple action d'opportunité, elle devient un axe fondamental de leur stratégie. Cette propagande numérique s'appuie notamment sur les réseaux sociaux de type *Facebook*, *Twitter*, *VKontakte*, *YouTube* ou encore *WhatsApp*, qui relaient des vidéos d'une extrême brutalité ou des articles biaisés. Dans ce contexte, les exécutions d'otages occidentaux en 2014 visent à ébranler les opinions publiques et la détermination des démocraties occidentales, à polariser les communautés. Cette politique de médiatisation de la terreur est aussi conduite contre les populations du Proche et du Moyen Orient pour les dissuader de toute velléité de résistance. Elle vise également à recruter des combattants étrangers provenant du monde entier en cherchant à exacerber leurs frustrations et à désinhiber leur soif de violence. Les images sont travaillées pour avoir un maximum d'impact sur les esprits. De nombreux analystes soulignent leur ressemblance avec le graphisme et la mise en scène de jeux vidéo du type de *Call of Duty*.[2] L'image s'accompagne d'un texte défilant chargé de marteler un message prônant la résistance à l'agressivité des infidèles. Des forums viennent ensuite conforter le message et "accompagner" le recrutement.

Une menace cyber prise au sérieux

Une initiative collective démontre avec quel sérieux la propagande numérique de Daech est considérée sur la scène internationale. En effet, le 27 octobre 2014, la création d'une coalition de l'information est annoncée. Elle regroupe les États-Unis, des pays européens (France, Royaume Uni, et d'autres) et des pays arabes (Arabie Saoudite, Égypte,

---

[1] Le procédé n'est pas nouveau en lui-même. La radio a souvent joué l'appel au meurtre : la Radio-Télévision Libre des Mille collines au Rwanda porte une lourde responsabilité dans le génocide de 1994.

[2] *Cf.* http://www.washingtonpost.com/news/morning-mix/wp/2014/10/28/the-islamic-states-call-of-duty-allure.

Émirats Arabes Unis…). Elle a pour mission de contrer la propagande et les actions de recrutement de *Daech* sur Internet. Si cette initiative se confirme dans les faits, elle viendra compléter concrètement les efforts déjà établis sur les plans militaire et financier.

Certains pays occidentaux sont déjà entrés dans cette lutte. La France a démontré un volontarisme fort en capacité de cyberdéfense dans sa loi de programmation militaire (LPM) de 2013. Dans son actualisation, elle évoque maintenant un "*dispositif de cyberdéfense militaire renforcé*". Dans le même mouvement, le Premier ministre français annonce la création d'une armée de modérateurs pour surveiller et étouffer la visibilité des réseaux djihadistes sur Internet.[3]

Si la bataille a donc bien commencé dans la couche sémantique, la couche logicielle n'est pas en reste.

L'attaque cyber dans la profondeur stratégique

Jusqu'ici, les conflits modernes nous enseignaient que l'attaque d'un adversaire dans sa profondeur stratégique pouvait être conduite par des raids aériens, des missiles de croisière ou des opérations commando très ciblées. La décision militaire repose alors sur la faisabilité technico-opérationnelle, sur l'impact politique souhaité (démonstration de force ou discrétion) et sur le niveau de prise de risque acceptable (défense anti-aérienne inviolable, capture de pilotes ou de commandos, etc.). Le cyber ouvre une nouvelle option.

La neutralisation à distance par attaque cyber

Le code *Stuxnet* est devenu un cas d'école. Après avoir longtemps menacé l'Iran de frappes aériennes sur ses centrales nucléaires, il semble reconnu aujourd'hui que les dirigeants américains et israéliens ont finalement préféré conduire une attaque informatique. Cette opération discrète leur permettait de ralentir le développement du nucléaire iranien en préservant (au moins temporairement) leur anonymat et en minimisant les risques physiques pour leurs propres forces armées. Dans les faits, le ver informatique *Stuxnet* était programmé pour agir sur les commandes des systèmes industriels d'enrichissement de l'uranium. Dans la durée, en changeant les vitesses, le code a leurré les ingénieurs superviseurs avec de fausses données, dégradé les centrifugeuses et neutralisé ainsi la production. Au final, le programme global aurait pris deux ans de retard.

La complexité de l'attaque ne porte pas uniquement sur le code malveillant en lui-même. Certes, ce virus se devait d'identifier les systèmes industriels puis de les reprogrammer en toute discrétion. Mais cette manœuvre porte en fait tous les attributs d'une véritable opération, avec ses phases de conception (analyse systémique de la cible), de préparation (élaboration de l'arme et mode de diffusion) et de conduite. En effet, pour atteindre les réseaux de commande des usines nucléaires de Bushehr ou Natanz, il fallait définir précisément le dommage attendu (l'état final recherché), procéder à une analyse renseignée des cibles, définir les modes d'injections possibles, même en *air gap* – c'est-à-

[3] *Cf.* http://www.lefigaro.fr/politique/le-scan/citations/2015/05/28/25002-20150528ARTFIG00071-valls-promet-un-bataillon-de-community-managers-contre-la-propagande-djihadiste.php.

dire dans ce cas, grâce aux clés USB –, permettre l'usurpation de signatures après vol ou recel de clés privées, des auto-sauvegardes, etc. Pour cela, il fallait aussi recourir à une ingénierie sociale permettant de miser sur des défaillances d'opérateurs ou des complicités internes. Enfin, pour le contrôle de l'opération, il fallait pouvoir contenir le virus afin d'éviter une contamination insurmontable en disposant d'un antidote ou d'une date d'expiration qui était, dans ce cas précis, le 24 juin 2012.

Le cyber : nouvelle pierre angulaire du renseignement

Les révélations d'Edward Snowden ont levé le voile pudique qui couvrait encore les activités d'espionnage des mondes cyber et électromagnétique. De nombreux aspects de l'existence de PRISM,[4] dans la continuité d'ECHELON,[5] étaient déjà accessibles mais les alerteurs passaient, au moins en France, pour de doux paranoïaques.

Depuis, la recherche du renseignement prend une apparence plus agressive… Par exemple, dans la continuité de *Stuxnet*, une attaque par un virus baptisé *Flame* est détectée en 2012, une nouvelle fois en Iran mais aussi en Syrie, en Arabie Saoudite et en Égypte. Bien que 20 fois plus gros, *Flame* possède de nombreuses similitudes de conception avec *Stuxnet*.[6] Il ne s'agit pas cette fois de neutraliser un système de contrôle et de supervision, mais de voler des masses de données stockées sur des systèmes d'information de gestion d'installations pétrolières du Moyen-Orient.[7] Il ne vise donc pas un système industriel de type SCADA[8] mais cible le système d'exploitation Windows de Microsoft. Ce virus "espion" très sophistiqué permet à son concepteur de recopier des fichiers en masse (plans d'organisation, plans d'architecture, schéma de construction, etc.) mais aussi d'opérer des captures d'écran, d'activer à distance des micros, de conserver des données de connexion *Skype*, les fonctionnalités *Bluetooth*. Il serait piloté à distance tant pour la maîtrise de sa propagation que pour l'orientation de sa recherche en renseignement. Comme *Stuxnet*, il disposerait d'une capacité d'obfuscation[9] et aurait fonctionné deux ans avant d'être détecté. Il pourrait d'ailleurs appartenir à une même famille de concepteurs, ce qui orienterait une nouvelle fois les soupçons vers les États-Unis et Israël.

Les raids hybrides dans la couche logicielle

Cette vision offensive de l'attaque cyber n'en est qu'à ses débuts. Dans le domaine de l'énergie, un nouveau virus, *Dragon Fly/ Havex/ Energetic Bear*, est révélé par la société

---

[4] PRISM est un programme américain, conduit par la NSA (National Security Agency), de surveillance électronique par la collecte de renseignements à partir d'Internet et d'autres fournisseurs de services électroniques, qui prévoit le ciblage de personnes vivant hors des États-Unis.

[5] ECHELON est le système mondial d'interception des communications privées et publiques (SIGINT) mis en place à partir des années 1970 par les États-Unis, la Grande-Bretagne, le Canada, l'Australie et la Nouvelle-Zélande.

[6] K.F. Morton & David Grace, "A Case Study on Stuxnet and Flame Malware", 10 septembre 2012 (mis à jour le 8 juillet 2014) : http://vixra.org/pdf/1209.0040v1.pdf.

[7] Cf. http://tzedek-tzedek.blogspot.fr/2012/07/whats-difference-between-stuxnet-flame.html.

[8] Le sigle anglophone SCADA (pour *Supervisory Control And Data Acquisition)* renvoie aux systèmes de contrôle et d'acquisition de données.

[9] Procédé par lequel un code est rendu difficilement pénétrable à la compréhension humaine, en empêchant une rétroconception rapide.

informatique Symantec à l'été 2014. Il infecterait depuis 2011 de grands groupes énergétiques américains et européens et pourrait perturber la distribution d'énergie. Son niveau de sophistication est tel qu'il est très probablement produit par un État qui aurait coordonné sa propagation. Comme *Stuxnet,* il s'attaque aux systèmes informatiques de contrôle et de supervision de type SCADA mais procède par une attaque indirecte en ciblant les maillons les plus faibles de la chaine de sécurité informatique : des sites Internet de sous-traitants et de fournisseurs. Ces derniers sont le plus souvent moins bien protégés ce qui les rend très vulnérables ; ce sont eux, via des téléchargements de mise à jour de logiciels utilisés par le système de contrôle et commande, qui favorisent la diffusion du virus. Selon les spécialistes, cette attaque très élaborée permettrait à la fois de récupérer des données et de saboter des systèmes de production. Elle serait donc une combinaison des attaques de type *Stuxnet* (dominante sabotage) et *Flame* (dominante espionnage). Difficilement traçable, l'offensive pourrait provenir de Russie selon certains médias ou sociétés de sécurité.

La bataille logicielle est donc aussi engagée, le plus souvent dans le secret. D'autres batailles traversent enfin la couche physique du cyber.

Le cyber investit le champ de bataille

L'informatique et l'électronique ont envahi le champ de bataille. Dans les armées modernes, tous les systèmes d'armes, de commandement, de renseignement, de navigation, de stockage et d'exploitation des données utilisés sont intrinsèquement cyberdépendants ! A l'ère de l'info-numérisation, cette tendance descend jusqu'à l'équipement du fantassin.

L'utilisation de toute cette haute technologie a bien entendu une finalité concrète ; elle vise avant tout à améliorer l'efficacité des armées modernes. En effet, elle favorise les appréciations de situation, aide à concevoir l'action et permet d'accélérer le processus de décision. Elle augmente la réactivité, car elle réduit les délais de diffusion des ordres jusqu'aux plus petits niveaux. Elle permet enfin de maîtriser la force en évaluant, au plus juste, la nature de l'attaque ou de la riposte nécessaire. En cela, le cyber devient le centre névralgique dans la bataille. Il devient donc une cible.

Le cyber à l'offensive… du politique au tactique

Le conflit Russie-Géorgie de 2008 incarne bien cette entrée du cyber dans la guerre classique. Les premières offensives russes se concentrent sur le niveau politique. Les sites Internet de la Présidence et du Parlement géorgiens subissent une vaste attaque informatique dès le 20 juillet 2008. Le gouvernement géorgien en est bien le centre de gravité, victime de déni de service distribué (DDoS),[10] de déroutement "malveillant" et de "défaçage".[11] Ces manipulations paralysent le pouvoir qui ne peut plus communiquer en

[10] Les agressions par DDoS appliquent la même méthode de *botnets* que pour l'Estonie : ces réseaux d'ordinateurs zombis dont les pilotes sont difficilement identifiables, répartis dans le monde entier et saturant simultanément les sites de leurs requêtes.

[11] Le "défaçage" consiste à transformer un site, ici pour discréditer le président Saakachvili, comparé à Hitler dans un montage photo sommaire.

interne avec sa population et son armée, comme en externe avec les médias étrangers ou les chancelleries pour obtenir des appuis internationaux.

Sur le terrain, les offensives cyber sont synchronisées avec les principales actions de combat dans les autres espaces physiques (terrestre, aérien, maritime). Offensive terrestre à l'Ouest, blocus naval, bombardement autour des ressources énergétiques et supériorité informationnelle par une domination cyber indiscutable semblent bien consacrer une victoire sous tous les aspects du combat moderne… Cette domination s'amorce aussi au niveau tactique où des localités précises sont virtuellement attaquées pour couper leurs capacités d'information avant et pendant les offensives de blindés ou des chasseurs bombardiers.

Cette perte totale de maîtrise de l'information, additionnée aux défaites tactiques et opératives, a conduit à une rapide défaite stratégique de la Géorgie. Sous pression internationale, le conflit a pris fin quelques semaines plus tard avec la signature du cessez-le-feu, le 15 août 2008.

Une manœuvre cyber multicouches

La participation désormais quasi systématique du cyber aux conflits est encore confirmée quelques années plus tard en Ukraine. Les modes d'action s'adaptent à chaque fois au contexte particulier du conflit et aux enjeux de puissance régionaux en combinant des démonstrations de force et des actions clandestines. Lors de l'occupation de la Crimée par la Russie puis des affrontements de 2014, des attaques coordonnées se multiplient sur toutes les couches cyber : physique, logicielle et sémantique. En effet, des dégradations physiques neutralisent des infrastructures de télécommunication en s'en prenant directement à des réseaux de câbles en Crimée. Dans le même temps, des attaques logicielles paralysent les sites parlementaires ukrainiens et ceux du Conseil de sécurité national. De nombreuses données personnelles et gouvernementales sont également récupérées par des groupes de *hackers* pro-russes, comme CyberBerkut.

Sur le terrain, les téléphones portables sont écoutés, localisés voire neutralisés favorisant des opérations de réglages de tir ou de ciblage. Enfin, des censures sont conduites sur les sites ukrainiens et des articles sont transformés en masse sur Wikipédia pour construire une autre lecture de l'histoire de la Crimée.

La maîtrise russe du combat cyber-électronique semble se confirmer. Cependant, cette approche tactique n'est pas isolée ; d'autres armées évoluent simultanément dans le même sens.

Vers le combat cyber-électronique

Lors de leur guerre en Irak, après de nombreux revers tactiques, les Américains ont été contraints à réadapter leur manœuvre en s'appuyant davantage sur le cyber. Ils sont parvenus à combiner l'agilité tactique des unités de guerre électronique déployées avec le soutien technique de la NSA, en particulier grâce à une mise à disposition de bases de données exploitables. Cet appui de la NSA se serait aussi étendu au piratage des systèmes

de communication des insurgés afin de prendre connaissance de leurs messageries, d'accéder à leurs téléphones ou de s'infiltrer dans des forums. En septembre 2004, les Américains développèrent une technique appelée *The find* pour localiser un téléphone même en veille. Ils ont alors réussi à ploter les résultats sur une carte.[12] Cette manœuvre cyber-électronique a permis de neutraliser ou d'arrêter plusieurs centaines d'insurgés. Par ailleurs, dans la même période, le développement du brouillage anti-IED a contribué à limiter le nombre d'attentats réussis. D'une manière encore plus élaborée, durant les années suivantes, les *hackers* américains envoyaient de faux messages aux insurgés (usurpation d'identité) en leur donnant un rendez-vous dans un lieu où des unités de capture les attendaient et saisissaient de nouvelles données essentielles de sympathisants d'Al-Qaïda ou d'autres factions : adresses e-mail, numéros de téléphone, identifiants techniques, vidéos, mots de passe...[13] Cette coordination tactique du cyber et de la guerre électronique a permis aux forces américaines de mieux comprendre leur ennemi et de leur infliger par la suite, sur renseignement, des nombreuses défaites. Le général Petraeus a estimé que cette capacité avait été déterminante dans le succès du "*Surge*" de 2008.[14]

Conclusion

Cette traversée des champs de bataille connus du cyber permet de mesurer avec quelle vitesse cette forme de combat est venue s'ajouter aux formes plus anciennes. Elle ne change pas les principes de la guerre mais elle ajoute de multiples modes d'action possibles. Elle impose d'ores et déjà une faculté d'adaptation permanente pour se mouvoir dans cette forme de combat évolutif. Nos ennemis le savent. En 2015, après avoir prôné une diffusion tous azimuts de données numériques à vocation de propagande, Daech met en place un code de "bonne conduite" sur Internet pour ses fidèles. Ce code précise les failles de sécurité susceptibles de fragiliser leur action et interdit les publications intempestives de photos et de documents qui permettraient de livrer des horaires, des localisations et des noms au service de renseignement de ses ennemis… Dans le même temps, le cyber Califat s'introduit sur TV5. Les cyber-batailles continuent.

---

[12] Shane Harris, *@WAR: The Rise of the Military-Internet Complex*, New York, Houghton Mifflin Harcourt, 2014.

[13] Eric Schmitt & Thom Shanker, *Counterstrike : The Untold Story of America's Secret Campaign against Al Qaeda*, New York, Times Books, 2011.

[14] Augmentation du volume des troupes américaines et allongement de la durée des rotations en Irak, décidés par le Président Bush en 2007.