

La cyberdéfense est d'abord un combat

BRENNUS 4.0

le lieutenant-colonel Le Dez, chercheur associé du pôle « Mutation des conflits » du Centre de recherche des écoles de Saint-Cyr

publié le 23/03/2020

Sciences & technologies

Tous les conflits armés actuels intègrent une part de combat dans le cyberspace. La cyberdéfense, domaine souvent méconnu, permet ce combat numérique qui est aujourd'hui indispensable pour dominer. Nous avons l'habitude de sécuriser nos systèmes d'information. La cyberdéfense est fondamentalement une autre mission dans un vaste espace numérique. Grâce au renseignement cyber à fin d'action, le combat numérique se planifie et se conduit en reproduisant une dialectique guerrière connue entre attaquants et attaqués.

Cyber défense et sécurité

La différence entre cyberdéfense et cybersécurité est de même nature que celle plus générale entre défense et sécurité dans les opérations militaires.

La défense ne se pense que dans l'interaction avec un attaquant. Elle permet les modes tactiques défensifs et offensifs si étroitement liés.

La sécurité, plus globale, apporte ce sentiment d'être protégé : rien ne doit priver le chef de sa liberté d'action, rien ne doit affaiblir sa force protection. La sécurité est aujourd'hui encadrée par des directives, réglementations, procédures, et certifications indispensables pour atteindre une cohérence globale.

Dans l'espace numérique, cette différence et ce continuum entre sécurité et défense existent aussi.

La cybersécurité prépare le terrain numérique, l'équipe, l'assainit, le transforme pour que le combattant y soit en situation favorable quand il détectera l'adversaire.

La cyberdéfense cherche le contact, première étape du combat, grâce au renseignement cyber à fin d'action. Une fois l'adversaire repéré, la cyberdéfense le combat pour réduire sa liberté d'action, parfois au-delà de nos lignes de front numériques, parfois par des actions en dehors du champ cyber. La cyberdéfense finit aussi la bataille par une phase

de stabilisation assurant la transition vers ceux en charge de la sécurité. C'est un conflit somme toute classique.

Le théâtre d'opérations cyber est bien plus vaste que nos seuls ordinateurs, ce n'est pas qu'un domaine informatique. Il englobe tous les équipements qui contiennent un peu d'électronique. L'abondance des objets numériques, connectés ou pas, tend à être la norme dans nos champs de bataille. Ils sont militaires et décuplent nos capacités de combat, notamment en échangeant des données pour construire une situation opérationnelle à jour, permettant ainsi l'accélération de la manoeuvre et du commandement. C'est la numérisation du champ de bataille.

Ils sont civils et nous accompagnent au quotidien dans notre vie privée qui ne s'arrête pas quand nous revêtons nos treillis. Ces objets civils sont aussi très utilisés par nos adversaires ; petits drones ou téléphones portables sont des cibles du combat numérique.

Ils sont industriels et nous ne les voyons plus. Ils permettent d'ouvrir une porte facilitant une infiltration commando, ils permettent de déjouer la surveillance ennemie en perturbant le bon fonctionnement des dispositifs d'alerte, ils renseignent sur l'utilisation de l'espace civil en y détectant des activités humaines.

Notre espace électronique intelligent, celui de tous nos systèmes d'armes, nos chars et nos canons, nos véhicules et nos drones, n'est pas un espace purement militaire. Pour des raisons de coût et de facilité de développement, ces systèmes militaires sont aujourd'hui de plus en plus construits avec les mêmes composants informatiques et électroniques que ceux que nous retrouvons dans les maisons et les entreprises et qui sont déjà la cible d'attaques cyber. Cela facilite le travail de l'attaquant, mais de la défense également qui agit en terrain connu.

Au-delà de ce seul aspect numérique, le théâtre d'opérations cyber englobe aussi toutes les informations qui y circulent et tous les humains qui y accèdent. Le combat cyber d'influence est un combat sur les perceptions. Il utilise le cyberspace, souvent loin de sa technicité, proche de sa puissance sociale, informationnelle et médiatique. Il touche directement les volontés.

Enfin, le théâtre d'opérations cyber englobe concrètement tous les équipements électroniques : exploser physiquement en mille morceaux une capacité cyber est la meilleure façon de la détruire.

Même si elle s'élargit à d'autres domaines notamment industriels, la cybersécurité est un domaine fondamentalement dédié aux spécialistes informatiques, aux ingénieurs et aux techniciens. Ils fournissent une ressource sécurisée de commandement et d'échange d'informations sans laquelle toute victoire paraît fragile. Luttant contre la pollution numérique, ils participent indirectement à la lutte permanente contre le brouillard de la guerre cyber. La sécurité est d'autant plus indispensable qu'elle a pour objectif d'ôter sinon de réduire la liberté d'action de l'adversaire dans notre cyberspace. C'est donc un facteur de puissance, un de ceux qui fait que l'on sera toujours plus fort dans notre cyberspace.

La cyberdéfense est le domaine des combattants numériques dont l'esprit est proche de l'engagement guerrier. Le combat numérique se pense, s'organise, se planifie, se conduit comme tous les autres. Il en tire des principes et des savoirs exploitables dès aujourd'hui. De même nature, il s'intègre facilement dans toutes les autres formes de combat avec encore cet obstacle, c'est un combat jeune et tout en découverte.

La sécurité doit être permanente alors que la défense réduite au seul combat est une phase courte. Comme en bien des choses, cette distinction n'est pas absolue, la préparation et le soutien de ses forces tendent à donner à la défense un caractère permanent. De plus, dans notre monde incertain, puisque la menace est constante, les missions de renseignement et de recherche de l'adversaire qui en découle sont aussi permanentes.

L'attaque doit être aussi possible à tous moments. Puisque le combat numérique reste encore sous le seuil de la guerre, il donne la possibilité aux chefs la permanence de l'action en vue d'affaiblir l'adversaire avant d'agir plus violemment.

L'indispensable renseignement à fin d'action numérique

Une phase de renseignement initie toute bataille. Le renseignement permet d'établir l'ordre de bataille, de caractériser l'adversaire. Il est vital de connaître sa forme numérique, ses modes d'action, les traces qu'il laisse ou les armes qu'il utilise pour pouvoir orienter les recherches dans un espace si vaste. Comme dans le combat terrestre où il est impossible de surveiller en permanence chaque itinéraire, il faut orienter ses capacités de détection avec des dispositifs statiques et dynamiques de recherche.

En défensive, la recherche de l'adversaire s'apparente à de la chasse (le terme hunting est celui utilisé par les combattants numériques). Ces patrouilles cherchent sur des équipements numériques les indices de présence ou de passage de l'adversaire. Le plus discrètement possible, ils fouillent dans les mémoires, dans les disques durs et les processeurs, dans les journaux d'événements de tous les équipements électroniques. Ils analysent les données, fichiers et flux réseaux anormaux. La discrétion permet de ne pas éveiller les soupçons de l'adversaire qui se terrerait s'il se savait recherché.

Le renseignement cyber est la composante qui permet la cyberdéfense. Sans cette capacité de renseignement à fin d'action, il ne s'agirait que de sécurité qui, imaginant un adversaire théorique, n'a d'autre solution que d'agir uniquement en conformité à des textes de réglementation et une étude de risque souvent datée.

Le renseignement est aussi obligatoire pour que tous les chefs tactiques et opérationnels s'approprient le sujet « combat dans le cyberspace ». Au niveau des combattants numériques, comme pour toutes les formes de combat, la technique règne (ainsi que les acronymes ésotériques). Souvent, le vocabulaire, la compréhension de la situation ou l'emploi des armes sont très techniques et parfois peu intelligibles pour des non-spécialistes. Or, s'il reste sous son aspect le plus technique, il est impossible pour un commandement de comprendre et d'intégrer le combat numérique, de le planifier et de le conduire dans toutes les autres formes de combat terrestre. Il faut traduire les informations techniques comme une adresse IP (information de base en combat numérique, et dont beaucoup de lecteurs naturellement ne comprennent ni la signification, ni ses enjeux) en une information du monde physique (un pays, une entreprise, une région, un groupe d'attaquants, une machine déjà utilisée par l'adversaire dans d'autres opérations, etc.). Cette transformation numérique/physique est aussi rendue possible par le renseignement tactique intégré dans les combats. C'est seulement si cette transformation est faite que le combat numérique peut échapper à son entre-soi et être enfin intégré comme une vraie capacité de combat. Cette traduction fonctionne aussi dans l'autre sens, d'un commandement non cyber vers le combat numérique.

Intégré dans les unités de combat numérique, le renseignement à des fins d'action est indispensable à la cyberdéfense pour combattre dans un cycle tactique court. Il est impossible de séparer cette capacité de renseignement et le combat en lui-même ; à

toutes les étapes du combat il y a obligation de renseignement.

La conduite et la planification du combat numérique

La recherche de l'adversaire est faite par des opérations planifiées avec des critères très assimilables à ceux du contrôle de zone par l'armée de Terre. A partir du renseignement, la planification séquence la chasse et coordonne les unités, détaille les modalités de recherche (qui, quoi, quand, où, comment, pourquoi, etc.). Cela peut nécessiter l'équipement du terrain numérique pour forcer l'adversaire à aller vers nos capacités de détection (une mission du génie numérique), temporairement canaliser les flux ou interdire des zones afin d'obliger l'adversaire à bouger pour faciliter sa détection. Il faut parfois montrer ostensiblement quelques manoeuvres de déception numériques pour générer de l'animation ennemie.

L'adversaire est découvert.

Tout comme dans chaque combat, c'est l'incertitude qui règne et il ne faut pas montrer que l'on a peut-être repéré une de ces positions.

L'adversaire est là, on le voit, on le surveille, on le suit, on cherche à comprendre qui il est réellement et ce qu'il fait, ce qu'il veut, quelles armes il utilise. Tant qu'il n'agit pas contre nous, nous avons plus intérêt à préciser le renseignement sur lui que de dévoiler nos intentions. Nous cherchons surtout à connaître l'ensemble de son dispositif, à connaître l'intégralité de son implantation, ses moyens de communication. Rien ne serait plus facile que d'agir tout de suite, rien ne serait moins efficace sauf s'il y avait un danger réel.

Nous savons que dès que l'on pénètre un système numérique, la première mission est d'y multiplier les positions et les chemins de transmission de données (les systèmes numériques sont instables et il faut consolider son dispositif d'attaque). Les positions ennemies peuvent être nombreuses et bien dissimulées, dormant et servant de secours. Puisque l'attaquant n'a d'autres solutions que de multiplier les voies de pénétration et d'exfiltration, avec des technologies et des camouflages différents, toute correction d'une vulnérabilité ne ferait que fermer une porte sans réduire l'attaquant. Forcément, s'il constate qu'il a été vu à un endroit, il va changer de mode tactique et il va camoufler son dispositif plus profondément. Il sera toujours là, juste avec des modes tactiques plus discrets et donc plus difficilement visibles pour le défenseur. Il pourra toujours agir, parfois brutalement alors qu'on ne le voyait plus. Pour éviter cela, le but à atteindre pour le défenseur est de connaître l'intégralité du dispositif ennemi pour être en mesure de le détruire.

Cette mission renseignement sur l'attaquant ne peut exister que si la maîtrise des systèmes est totale. C'est là encore une affaire de continuum sécurité – défense. Des sonnettes fixent les lignes rouges que l'attaquant ne doit pas franchir, des actions qu'il ne doit pas faire. La planification et l'ordre tactique qui en découle préparent la réponse à tout changement de posture de l'attaquant. Cela peut passer par son éviction quand bien même il n'a pas été possible de découvrir l'intégralité de son dispositif.

Mais cette phase d'acquisition du renseignement n'est pas non plus que contemplative. Elle doit permettre de renforcer certaines positions sans que cela soit vu comme une réaction face à une attaque. Elle doit aussi permettre la création de dispositifs de leurre logiciel pour attirer l'attention de l'attaquant et lui faire révéler ses intentions, sa tactique et ses techniques. Le leurre est également informationnel en l'intoxiquant, tout en lui faisant télécharger des codes qui facilitent l'acquisition du renseignement en retour. Le défenseur doit parfois aussi devenir attaquant.

Un dispositif de leurre (« pot de miel » simulant un équipement ou « bac à sable » pour tout un environnement numérique) est une portion simulée de terrain numérique faite pour se renseigner sur l'action de l'adversaire. L'adversaire y manoeuvre comme s'il s'agissait d'une portion de notre vrai cyberspace, interagissant à la fois avec ses bases d'attaque, à la fois avec d'autres positions dans nos réseaux. Le but à atteindre du défenseur est d'avoir suffisamment de connaissance du dispositif adverse en vue de couper définitivement toutes ses lignes de communication et supprimer ses positions dans notre cyberspace. Cette mission de renseignement nécessite aussi de canaliser l'ennemi dans cette nasse en disposant des obstacles ailleurs, notamment des lignes d'arrêt que sont les dispositifs de filtrage de flux réseaux (un combat de contre mobilité). La mission est bien de jalonner la manoeuvre de l'adversaire et de recueillir du renseignement en vue de porter le coût d'arrêt nécessaire en faisant le maximum d'attrition sur ses capacités de combat. Pouvoir surveiller l'adversaire en permanence sans être vu est fondamental, le camouflage des missions et dispositifs de surveillance est de mise. Il s'agira, comme dans tous les combats, de repérer les faiblesses de l'adversaire pour pouvoir y appliquer la force juste et nécessaire au bon moment pour le vaincre.

Action – réponse, c'est un dialogue qui s'installe entre les deux belligérants, un jeu de dupe car chacun pense que ses missions n'ont pas été décelées par l'autre. Le défenseur n'est pas obligé de rester dans son propre espace. La légitimité de ce combat est de passer à un moment dans un mode tactique offensif pour conserver l'initiative et être complètement maître du tempo. Comme dans toutes les formes de combat, ce continuum offensif-défensif devra être la normalité dans l'espace de bataille numérique.

Renseignement, planification, conduite : un état-major tactique de cyberdéfense est un état-major « normal » si bien connu dans nos armées. Il se construit autour de ces fonctions de base sans oublier l'absolue nécessité d'avoir une logistique, sans quoi rien n'est possible. Ainsi, il n'est pas difficile de penser son intégration dans la manoeuvre militaire globale puisqu'il en suit les principes, l'organisation, la volonté, l'esprit guerrier.

Titre : le lieutenant-colonel Le Dez, chercheur associé du pôle « Mutation des conflits » du Centre de recherche des écoles de Saint-Cyr

Auteur(s) : le lieutenant-colonel Le Dez, chercheur associé du pôle « Mutation des conflits » du Centre de recherche des écoles de Saint-Cyr

Date de parution 17/03/2020

EN SAVOIR PLUS
