Search and destroy

Ou l'art de la guerre technologique

Difficile désormais de représenter un capitaine Kronenbourg avec du bide et des jurons de forain pleins la poire comme au temps de la conscription. Les soldats sont des robots, des unités d'élite, des geeks. Si la guerre se déréalise, sa représentation aussi, et la critique anti-militaire peine à toucher sa cible. Rendons-nous la tâche plus concrète : voyons qui fait la guerre du XXIe et comment (matériels et doctrines).

Dans un contexte de resserrement du budget de la Défense, celui de sa Recherche & Développement augmente pour atteindre 1,5 milliard d'euros par an jusque 2019 : bourses de thèses, subventions à des labos, des PME et des industries. Renseignements électroniques, drones d'attaque et de surveillance, combattants « augmentés », armes cybernétiques font la guerre d'aujourd'hui. Sous la double impulsion de la technologisation des forces et de la transformation des ennemis sur le mode « asymétrique », l'art de la guerre évolue.

Boule de crystal électronique

Dans la critique anti-militaire ou celle des armes de maintien de l'ordre, la *stratégie* et le *renseignement* en représentent souvent un point aveugle. Elle est pourtant la base de toute opération guerrière ou contre-insurrectionnelle : relevés topographiques, auditions, indics, infiltrés, interceptions radio et électroniques. Quand la France annonce ses velléités d'attaquer la Syrie en 2013, elle commence par envoyer une frégate d'interception et des drones de surveillance. Il en va de son *indépendance stratégique* vis-à-vis des États-Unis.

Avec les révélations d'Edward Snowden, on mesure à quel point le renseignement se technologise : « Le développement des activités du renseignement dans le domaine cyber [...] doit permettre de mieux identifier l'origine des attaques, d'évaluer les capacités offensives des adversaires potentiels et, si nécessaire, d'y répondre » souligne la Loi de Programmation Militaire de 2013. Ainsi le renseignement a-t-il fait l'objet d'une attention prioritaire malgré un budget global resserré : achat de satellites de renseignement électromagnétique et de reconnaissance optique, avion de guerre électronique, drones tactiques, avions légers de surveillance et armes de cyberguerre.

Si le nombre total de militaires est en baisse depuis plusieurs années, ceux du renseignement sont en hausse constante. Parmi les 430 nouvelles recrues de la DGSI (ex-DCRI), la moitié sont analystes, linguistes ou ingénieurs en cyberdéfense. Les services de renseignement militaire ont été renforcés par l'arrivée de 300 spécialistes du renseignement électronique. Et la moitié des 6 000 agents de la DGSE sont préposés à l'interception des télécommunications.

Ce n'est pas tout d'intercepter des données, encore faut-il les analyser. « Le véritable enjeu économique et technologique, pour lequel tout est à construire, est le traitement automatisé des données dont la quantité ne cesse de croître » réclamait la DGSE auprès des députés.[1] Début 2013, le campus

1 *La Voix du Nord*, 21 février 2014.

universitaire de Saclay, au sud de Paris, et la fleur du « complexe militaro-informatique » ouvraient un programme de recherche dédié à l'exploitation algorithmique des données brutes (textes, images, vidéos, réseaux sociaux, SMS, mails) aspirées dans le « Big Data ».[2] Ce projet est baptisé « iMMENSE ». Deux membres du Commissariat à l'énergie atomique dont l'un est détaché à la DGSE y pilotent les fleurons de l'industrie française.[3] Armée, recherche, industries montent au front de la guerre électronique.

Du soldat-robot…

Avant que les attentats islamistes n'influent sur la politique militaire française, les seules capacités humaines renforcées par la LPM étaient les forces spéciales, ces petites unités autonomes et entraînées aux actions de choc, ciblées, rapides, légales ou non (cf. Libye), en territoire ennemi. Les efforts de recherche se porteront donc désormais sur « l'amélioration [du] capital humain » et de son « cerveau-machine », pouvait-on entendre lors d'un colloque tenu à l'école militaire le 9 juin 2015, regroupant médecins et officiers.[4] Tout le monde connaît désormais les exosquelettes, ces carapaces qui permettent aux soldats de porter des charges lourdes sur de longues distances. Les dernières trouvailles scientifiques vont vers l'aide à la prise de décision si ce n'est le téléguidage des combattants.

Depuis les années 1980, les armées ont enclenché la « Numérisation de l'espace de bataille » (NEB). C'est l'Internet appliqué aux fronts. Exemple : l'entreprise française Bull travaille sur le programme « Scorpion », piquer pour tuer.[5] Le combattant « FELIN », géolocalisé et bardé de capteurs, est en « communication » avec le char Leclerc. Un drone passant par là prévient l'hélicoptère Tigre qu'une menace est imminente. Il propose au combattant d'envoyer une salve appuyée. Le drone constate la mort de l'ennemi et calcule le nombre de balles restant dans le Famas du fantassin. Soldats-robots et robots-soldats parlent le même « langage » numérique. C'est la guerre des machines, le crime assisté par ordinateur, l'aide au tir rationalisée, la connaissance « en temps réel » des pertes humaines et matérielles, ou encore l'aide au pilotage grâce à la réalité augmentée.

…au robot-soldat

Avec les drones ou les outils de renseignement numérique, un « opérateur humain » reste dans la « boucle de décision ». C'est encore trop. Il éprouve de l'empathie pour ses victimes, se fatigue, tombe malade, est sujet à des « syndromes de stress post-traumatique » dont notre système de sécurité sociale se passerait volontiers. Les armées travaillent donc sur des robots létaux autonomes (RLA) programmés pour « sentir-penser-agir » sans l'aide d'un humain. Les capteurs et caméras analysent les situations (Sentir). Les processeurs (une intelligence artificielle) décident de la réaction selon les *stimuli* captés (Penser). Et des « effecteurs » exécutent les décisions (Agir : tirer, exploser). C'est le cas des missiles anti-missiles Phalanx qui engagent automatiquement des menaces selon les observations faites par les radars. Ou des mitrailleuses dotées de caméras et capteurs de chaleur développés par Samsung, et déjà utilisés par la Corée du sud pour contrôler sa frontière nord.

Le temps de décision nécessaire aux robots-tueurs étant inférieur à quelques

2 *Guerres dans le cyberespace, services secrets et Internet*, Jean Guisnel, La Découverte, 1995, rééd. 2013.

3 Côté entreprises : Alcatel-Lucent, Alstom, Bull, Cap Gemini, EADS, EDF, Engie, Orange, PSA, Renault, Thalès ou Valeo. Côté Recherche :INRIA, CEA, Polytechnique, Supélec, CNRS, etc.

4 « L'armée à la recherche du "soldat augmenté" », *Le Monde*, 11 juin 2015.

5 *La Tribune*, 19 avril 2013.

nanosecondes, l'humain n'a plus la capacité d'intervenir. Constatant les « progrès » réalisés dans la vitesse de calcul, plusieurs ONG chapeautées par Human Rights Watch ont lancé en 2013 une campagne pour l'interdiction des « robots tueurs ». En effet, ces « RLA » posent un certain nombre de problèmes « éthiques » comme le contrôle de légalité. Quelle responsabilité humaine ou étatique reste-t-il ? Comment les capteurs peuvent différencier les civils des militaires, les combattants des non-combattants, notamment dans le cas des conflits avec des groupes non-étatiques ? Que devient le contrôle de « proportionnalité » interprété juridiquement comme le « bon sens » et la « bonne foi » d'un « chef militaire raisonnable »[6] ? Un robot est-il capable de « capter » un belligérant se rendant de lui-même ? Autant de questions posées par le droit des conflits armés que résoudront, car il ne faut jamais désespérer, les ingénieurs : ils ajouteront un jour une « couche d'éthique artificielle » à leurs créations morbides.

Guerre dans le cyberespace

Le réseau cybernétique est devenu le cinquième champ de bataille après la terre, l'air, la mer et l'espace. Le « tournant » de la cybersécurité française a lieu en 2008 avec la publication du *Livre blanc* de Sarkozy. Une Agence nationale de sécurité des systèmes d'information (ANSSI), sorte de NSA à la française, « a la charge, en cas d'attaque informatique majeure contre la Nation, d'organiser la réponse et de décider des premières mesures urgentes à faire mettre en œuvre par les administrations. »[7] Les 7, 8 et 9 février 2012, le premier ministre lançait le premier exercice « Piranet » – l'équivalent « cyber » des plans Piratox, Piratmair, Piratair ou Vigipirate. Outre les services de l'État, ceux de la santé, des transports et des communications électroniques étaient mobilisés : « Aujourd'hui, un virus informatique peut s'attaquer à une centrale nucléaire, à un barrage, à notre réseau de transports, faire dérailler un train ou attaquer la Banque centrale. Avec l'interconnexion, on peut mettre en l'air toute l'organisation sociale » entendait-on lors du Forum international de la cybersécurité en 2013.

Le financement des recherches consacrées à la cyberdéfense, *via* la Délégation générale à l'armement (DGA), a triplé en quelques années. Des filières universitaires s'ouvrent à la hâte pour former des ingénieurs en sécurité des réseaux, à Saint-Cyr, l'École militaire des transmissions, l'université Bretagne-sud, et même à l'IUT de Maubeuge (59).[8] Du côté des industriels, Cassidian cybersecurity ou Thalès réservent désormais 20 % de leur budget de Recherche & Développement à la sécurité informatique, contre 10 % dans les moyens de défense plus « classiques ».[9] La filière française se structure, les gros mangent les *start up*, et les contrats d'exportation font la gloire de la France : « Thalès participe à la protection des systèmes de défense de 50 pays, dont 25 membres de l'Otan. [...] Cassidian, la branche défense et sécurité d'EADS, fournit un centre opérationnel de sécurité à l'armée britannique »[10] La cyberguerre est un marché en explosion que le Plan d'Emmanuel Macron pour une « Industrie du futur » soutint publiquement en son temps.

Conséquences sur l'art de la guerre au 21ème siècle

Search and Destroy est une doctrine mise au point par l'armée américaine au Vietnam, popularisée en chanson par les *Stooges*, et remise au goût du jour par les fabricants d'anti-virus informatiques. La guerre froide vit se développer la dissuasion nucléaire, la

6 *Damoclès* n°142, 2013.
7 *La cyberdéfense : un enjeu mondial, une priorité nationale*, dit aussi « Rapport Bockel », juillet 2012.
8 lavoixletudiant.com, 28 février 2013.
9 *L'Usine nouvelle*, 29 janvier 2013.
10 *L'Usine nouvelle*, 29 novembre 2012.

guerre asymétrique[11] accéléra la technologisation des conflits. Si la bombe atomique polarisa le monde en deux super-blocs, la guerre technologique s'adapte aux conflits asymétriques, organisés sur un mode réticulaire, et dont la bataille contre l'État islamique est un modèle du genre. C'est pourquoi des voix d'anciens officiels (ministres, généraux, etc) se sont élevées ils y a quelques années pour stopper le programme nucléaire français. Pour de timides raisons éthiques, certes, mais surtout parce que le nucléaire serait le symbole coûteux d'une guerre d'un autre âge. La Stratégie nationale de sécurité des États-Unis de 2015 considère d'ailleurs que ses principales menaces proviennent désormais de « groupes [terroristes] », d'« États fragiles et affectés par des conflits », ou du « danger de cyber-attaques », plus que d'une guerre ouverte avec une puissance nationale.[12]

Nous retiendrons ceci quant à l'art de la guerre élevé à son stade technologique :

Une augmentation des effectifs de commandement, d'état-major et de renseignement. En 1945, un militaire sur vingt occupait une fonction de commandement dans l'*US Air Force*, désormais, on est à un officier de commandement pour quatre militaires.[13] La guerre postmoderne est affaire de stratégie plus que de force brute. Ce qui entraîne le concours de plus en plus appuyé de compétences « civiles » pour le maniement et l'élaboration des nouvelles armes.

Le privilège accordé aux attaques ciblées sur des centres stratégiques (centres de commandement adverses par exemple) et au bombardement aérien (drones ou avions). Et donc, la limitation du déploiement de troupes au sol. Ce qui a pour conséquence une limitation des pertes humaines et matérielles. Exemple : après 78 jours de bombardement du Kosovo par les pays de l'OTAN, aucune perte humaine en opération n'a été relevée du côté de l'Alliance et seulement deux avions ont été abattus. Soit l'équivalent d'un vingtième des pertes subies au Vietnam. Avec l'appui des Forces spéciales,[14] place au renseignement et aux frappes à distance, aux combats rationalisés, ciblés, efficients.

Plus technologique et moins humaine, la guerre se déroule de plus en plus dans en zone grise mi-humaine mi-machine, mi-légale mi-illégale. Tout cela entraînant sa déréalisation, quand bien même elle embarquerait avec elle journalistes et photographes. Elle est lointaine, ciblée, engage peu d'humains et dure le temps d'un éclair. Le viseur de la critique anti-militaire se resserrera sur les chercheurs et ingénieurs de la guerre si elle ne veut manquer sa cible.

TomJo, Janvier 2017.

11 Guerre dans laquelle des forces étatiques sont confrontées à des forces non-étatiques.

12 paul.quiles.over-blog.com

13 *Questions internationales* n°73-74, mai-août 2015,

14 Dans son budget 2015, l'US Army annonce que ses effectifs passeront de 520 000 à 450 000 pendant que ceux des forces spéciales augmenteront de 3 700 à 70 000. Cf. defense.blogs.lavoixdunord.fr, 25 février 2014.