La guerre « rustique » : du *KO* technique… au *knock-down* ?

Éric POURCEL | Docteur en droit, officier réserve opérationnelle.

L'étymologie latine du mot « rustique » nous apprend que ce terme est viscéralement lié à la campagne (*rus*), un milieu dont on considère que les conditions de vie sont simples, dures et détachées de tout confort par opposition à l'*urbs* romain, la ville qui représente sous Rome le lieu par excellence de la modernité voire de la civilisation.

Les outils de la guerre connaissent depuis le premier silex taillé une évolution univoque, celle d'une technicité toujours plus approfondie avec pour triple conséquence : la conquête de tous les milieux et la création même de nouveaux milieux comme le cyberespace ; une efficacité et des performances toujours plus redoutables conformes à la devise olympique, « *Citius, altius, fortius* » ; enfin, des coûts en croissance exponentielle au risque d'un épuisement économique.

VOCABULAIRE

Rustique (étymologie) : provençal, *ruste* et *rustic*, *rostic* ; catalan, *rustic* ; espagnol et italien, *rustico* ; du latin, *rusticus*, qui vient de *rus*, campagne. *Rusticus*, avec l'accent sur ru, avait donné *ruste*, *ruiste* ; rustique a été refait sur le latin au XIV^e^ siècle (https://dicocitations.lemonde.fr/definition_littre/38857/Rustique.php).

KO : Acronyme signifiant « *knock-out* », c'est-à-dire la mise hors de combat de l'adversaire dans le domaine de la boxe.

Knock-down : Terme utilisé en boxe lorsqu'un boxeur se relève dans les 10 secondes qui suivent sa mise à terre suite à un coup porté par son adversaire.

De la dépendance au progrès technique au *KO* technique…

Cette évolution a pour conséquence d'obliger les États à entrer dans une course sans fin, celle de la recherche d'équipements innovants afin de préparer la guerre de demain leur permettant d'avoir un temps d'avance sur leurs ennemis (cf. *RDN* n° 810, mai 2018) *. Ceux qui ne concourent pas, décrocheront et ne seront plus considérés comme des puissances respectées ; ils seront des États vassaux au sein d'alliances militaires ou des États de seconde zone dominés et sujets à des troubles politiques intérieurs. Pour les États messianiques et pour ceux

* Dossier « Préparer demain : concevoir et imaginer », notamment – et entre autres – BERNIER Jérôme, « Emploi opérationnel de l'intelligence artificiel », p. 12-18.

soucieux de leur indépendance, cette course crée une dépendance incontournable au progrès technique. Toutefois, jusqu'à récemment, cette dépendance s'inscrivait dans la mise en œuvre d'armements conçus, fabriqués et manœuvrés, ou, à tout le moins, contrôlés par l'homme.

La Dronisation et la robotisation intelligente des armées ou DRIA (cf. notre ouvrage, 2018) changeront graduellement et rapidement la donne : pour des raisons tenant à vulnérabilité des liaisons de communication et donc d'efficacité, notamment le temps de réaction (réactivité), le principe moral l'homme dans la boucle finira par être réduit aux acquêts, celui du contrôle afin de destruction d'un système d'arme automatisé déficient ou corrompu *. Pour des raisons sociales, l'exigence schizophrène de l'opinion publique du « zéro mort » à la guerre, le retrait de l'homme de la manœuvre des équipements dronisés et robotisés s'imposera inexorablement. À n'en pas douter, la course actuelle à la DRIA impactera la stratégie militaire pour voir apparaître une phase de la guerre techniquement paroxystique pendant laquelle seront opposés des moyens techniques à d'autres moyens techniques équivalents sans que l'homme ne soit engagé sinon intellectuellement, par la définition d'objectifs, et physiquement par le fait simple d'appuyer sur un bouton de départ des équipements. Ainsi, demain, à la différence de guerres qui comme en ex-Yougoslavie (1991-2001) ou en Irak (1991) ont causé de nombreuses pertes humaines, il existe un scénario probable d'une confrontation militaire dont l'objectif premier sera de paralyser les moyens de l'ennemi afin d'obtenir le *KO* technique.

Le *KO* technique pourrait être la résultante d'une stratégie de guerre ** se déroulant en trois phases fulgurantes :

- **Une phase de neutralisation des liaisons** communication, des réseaux et systèmes informatiques, électroniques et électriques militaires et civils névralgiques afin de créer un chaos sociétal brutal et inattendu. Se combineront à cet effet, après un temps de planification des opérations :

  – des actions de cyberattaque – dont l'efficacité peut être redoutable – des systèmes informatiques centraux et délocalisés (cf. Erwan ROLLAND, p. 195) affectant le *hard* et le *soft power* de cibles prioritaires vitales (serveurs centraux des centres de production d'énergie électrique, des ports, aéroports, etc.) ;

  – des actions de guerre électronique *via* l'emploi notamment d'armes à énergie dirigée électromagnétiques ou AED-EM (cf. lieutenant-colonel HENKE)

* Ainsi, « Le responsable des acquisitions de l'armée américaine (Bruce Jette) a déclaré (…) que le seul moyen de vaincre les armes de l'ennemi était de permettre à l'intelligence artificielle de contrôler certains systèmes d'armes. L'armée américaine a adopté l'IA, affirmant que les États-Unis ne peuvent pas rivaliser avec des adversaires potentiels tels que la Russie et la Chine sans la technologie futuriste. » in COX Matthew, « L'armée examine les armes contrôlées par l'IA pour lutter contre les tirs ennemis », *Military.com*, 10 janvier 2019 (www.military.com/).

** Ne sont pas compris dans ce descriptif, le temps de travail fondamental amont du renseignement militaire qui est permanent ni celui de la planification des opérations.

voire d'explosions nucléaires limitées en haute altitude dont l'objectif sera d'endommager en sus l'électronique qui conditionne le fonctionnement des installations civiles définies comme objectifs prioritaires et des armes au sens large, des réseaux de radars aux systèmes de défense du territoire en passant par les vecteurs tels que les missiles embarqués mais aussi leurs vecteurs porteurs (avion, bâtiments de surface, etc.) dotés d'électronique ;

– enfin des actions de neutralisation des systèmes de communication satellites soit par cyberattaque, par AED-EM ou par destruction directe *via* le tir de missiles ou l'emploi de lasers en position géostationnaire (cf. notre article, *RDN* n° 761, juin 2013).

- **Une phase de confrontation conventionnelle armée** tout milieu entre le reliquat des drones et robots intelligents (aériens, spatiaux, maritimes) encore opérationnels malgré la première phase, afin de neutraliser/détruire totalement le reliquat du « cheptel » des Systèmes d'armes létaux autonomes (Sala) d'un des deux belligérants ou groupes de belligérants situés au principal en zone internationale.

- **Une phase de projection et d'occupation du territoire** de l'ennemi défait par le *KO* technique qui pourrait se décomposer en deux temps :

  – un temps de neutralisation des moyens terrestres (Sala et autres équipements) encore en fonctionnement et infrastructures vitales (centre de production des armements, dépôt des réserves stratégiques de pétrole, etc.) sur le territoire de l'ennemi *via* l'application de l'*Air Land Battle*, suivi de la projection de moyens robotisés chargés de réduire les poches de résistances les plus importantes et les plus difficiles notamment en zone urbaine au gré d'objectifs prédéfinis ;

  – un temps d'occupation par des moyens humains et d'équipements dirigés par des hommes soutenus par des moyens dronisés et robotisés IA (cf. « Autonomie et létalité en robotique militaire », *Cahier de la* RDN).

Ce scénario fiction en trois phases n'est assurément pas un absolu mais il met en évidence qu'un État qui aurait investi dans le tout technique, *a fortiori* s'il n'investit pas ou pas suffisamment, qu'il soit doté ou non de l'arme nucléaire dès lors que les missiles à tête nucléaires ou les vecteurs qui les emportent seraient informatiquement corrompus ou électroniquement endommagés, se verra défait, au plus tard, à l'issu de la deuxième phase. Au plus tard en effet, car la première phase d'un tel conflit qui se limite à l'usage de moyens techniques visant finalement à corrompre l'informatique et à détériorer l'électronique de tous les systèmes ciblés (équipements militaires et civils névralgiques de l'ennemi) pourrait déjà suffire à désorganiser la défense d'un État pour l'obliger à accepter la cessation des hostilités.

Le *KO* technique pourrait ainsi se traduire par un chaos total, civil et militaire, de l'un des belligérants qui aboutirait non seulement à la neutralisation des centres de commandement et des équipements dronisés et robotisés mais aussi à la désorganisation de points vitaux comme les réseaux civils de télécommunications (informatiques et téléphonie), les centrales de production d'énergie électrique, les plateformes et réseaux de transports (aéroports, ports, ligne de chemin de fer, de métro, de tramway…), les systèmes informatiques bancaires… On peine naturellement à imaginer le niveau de désordre et de panique que pourrait créer une puissante attaque de nature électro-informatique concentrée sur des moyens de vie courante qui sont tous vulnérables.

Articulée avec la deuxième phase qui doit permettre d'interdire toute capacité de l'ennemi à attaquer son propre territoire, ces deux premières phases d'un conflit doivent ramener l'État défait à un âge de fonctionnement proche du milieu du XIX^{e} siècle ; toutefois, au milieu du XIX^{e}, la société était, elle, pensée et organisée logiquement et spontanément en adéquation avec son niveau de développement, les deux facteurs se déterminant mutuellement. Ici, le choc viendrait de la paralysie d'un État qui n'aurait pas prévu de modes alternatifs de fonctionnement ou de solutions provisoires alternatives à l'échelle de l'ensemble de son territoire et dans quasiment tous les domaines.

Après application de la troisième phase qui aboutirait à la destruction, et non pas simplement à la neutralisation, de nombre d'équipements militaires et installations civiles, c'est à l'âge de pierre que reviendrait l'État totalement défait.

Du *KO* technique au *knock-down*…

Cette hypothèse d'école supposerait que les États fassent preuve d'anticipation et se préparent à des modes alternatifs de fonctionnement dont la caractéristique essentielle serait d'être rustique mais très rapidement opérationnelle. Si un État défait peut toujours vouloir résister, et l'histoire démontre que cela est possible, si la guérilla peut être une réponse première à une défaite fulgurante, cela reste cependant des réponses insuffisantes : pour assurer une résilience, un État devrait définir et disposer, d'ores et déjà, des outils du *knock-down* tant sur le plan civil que militaire, c'est-à-dire des outils qui vont lui permettre de dépasser le temps de stupéfaction tenant à la situation de saturation en dysfonctionnement et neutralisation qu'il connaît en un temps extrêmement court.

Sur le plan civil, aucun Opérateur d'importance vitale ou OIV (définis par l'article R.1332-2 du Code de la Défense) ne peut désormais fonctionner sans électricité ni informatique, autant de raisons qui ont amené la France à inscrire dans sa Loi de programmation militaire (LPM) 2014-2019 que l'État doit assurer une sécurité suffisante des systèmes critiques des OIV, notamment les systèmes d'exploitation informatique. Pour autant, les obligations imposées aux OIV et à

l'État pour ce qui concerne la France en temps de paix sont-elles suffisantes pour permettre à ces acteurs fondamentaux de l'économie de se relever et à la France d'assurer son *knock-down* en cas de guerre non objectivement létale et visant au *KO* technique ? Rien n'est moins sûr puisqu'il n'existe pas l'équivalent d'un plan « Orsec » au regard d'une situation de *KO* technique en conséquence d'une action de guerre.

Par ailleurs, sur le plan militaire, le *knock-down* n'est envisageable que si en parallèle de l'acquisition des moyens hypersophistiqués que sont les drones et robots dotés d'IA, l'on conserve des savoirs « primaires » comme savoir s'orienter sans géolocalisation, savoir décider dans le brouillard de la guerre à partir de simples cartes d'état-major, se fondre dans un milieu en ignorance de toute information sur l'ennemi, se déplacer et développer des moyens de défense simples tant en termes de communication que d'armements manœuvrés par l'homme. Si le mot rustique vient à l'esprit, il faut alors l'entendre comme une armée capable de s'adapter, d'opérer et d'agir pour défendre le territoire sans satellites, sans drones et robots, sans communications électroniques, etc., ce qui suppose de disposer sans délai des moyens à cet effet. Y pensons-nous ? Serons-nous capables de réagir pour nous défendre ou devrons nous subir un armistice comme en 1940 ?

Ainsi, comme le souligne le général Beaufre « si à l'action planifiée succède vite la réaction, donc d'adaptation, l'une des qualités majeures des chefs comme des dispositifs », ce dernier va plus loin dans sa « stratégie de l'action » ; il considère que, puisque l'action militaire est constituée d'une série d'actes dont chacun peut être mis en échec par les réactions adverses, le problème consiste surtout à prévoir les contre-réactions qui pourraient être opposées à l'adversaire pour maintenir l'action dans le sens voulu, c'est ce qu'il appelle les « manœuvres contraléatoires » (cf. général DESPORTES, *Décider dans l'incertitude*, p. 84). Or, ici les manœuvres contraléatoires ne sont pas simplement une adaptation à la situation donnée, elles supposeraient en amont une anticipation certaine d'une situation inédite, celle d'un pays en situation de chaos majeur technique tant sur le plan civil que militaire, le tout en conformité avec le droit international humanitaire : les manœuvres contraléatoires ne seraient donc possibles que si l'on mettait les moyens financiers en cohérence avec ce qui relève d'un scénario hypothétique et coûteux.

Et pourtant, ainsi que l'a déclaré en substance le major général de l'Armée de terre, le général Barrera, lors de la clôture de la session 2018 de l'ESORSEM (École supérieure des officiers de réserve spécialistes d'état-major), il faut nous préparer simultanément à deux guerres, « La guerre des étoiles et la guerre Madmax ». Et c'est indubitablement un défi majeur que de penser deux guerres selon deux logiques antagonistes : l'une à la pointe des sciences où s'articulent les dernières avancées techniques dont le dénominateur commun sera l'IA et l'autre à la pointe du vouloir et du savoir au gré d'outils obsolescents mais subitement pertinents dont le dénominateur commun et l'élément de puissance seront l'Homme.

Éléments de bibliographie

Centre de recherche des Écoles de Saint-Cyr Coëtquidan (dir.), « Autonomie et létalité en robotique militaire », *Cahier de la* RDN, 2018 ; 264 pages (https://fr.calameo.com/read/000558115a2727297e70a).

Desportes Vincent, Décider dans l'incertitude, Économica, 2004, 200 pages.

Henke Gabriel, « Les armes à énergie dirigée électromagnétiques : la guerre électronique 2.0 ? », *Penser les ailes françaises* n° 37 « Décision politique et stratégie aérienne », 2018, p. 71 et suiv (lien).

Pourcel Éric, *Dronisation et robotisation intelligente des armées : de la dynamique conflictuelle et opérationnelle mixte homme-machine… à la dynamique conflictuelle et opérationnelle machine IA-machine IA ?*, Édition L'Harmattan, octobre 2018, 148 pages.

Pourcel Éric, « La révolution fulgurante : plaidoyer pour le laser en position géostationnaire », *RDN* n° 761, juin 2013, p. 32-36.

Dossier « Préparer demain : concevoir et imaginer », *RDN* n° 810, mai 2018.

Rolland Erwan, « Révolution numérique : vers une armée numérique ? », *Les Cahiers de la* RDN « Penser demain », 2017, 66e session du CHEM, p. 192-204 (https://fr.calameo.com/books/00055811559bb60c3f850).

ericpourcel4@gmail.com