Stratégie et réseaux dans la conduite des opérations militaires

Capitaine Djammel Metmati

Décembre 2014 - Article V.2

La convergence des réseaux humains et techniques influe sur la conception, la planification et l'exécution d'une opération militaire. Alors que la plupart des armées mondiales se structurent sur des modèles d'intervention, leurs déploiements s'appuient sur des principes liés aux caractéristiques des réseaux. Leurs engagements impliquent une maîtrise des élongations pour assurer la coordination des unités et une domination temporaire du cyberespace face à des adversaires potentiels. Cet art opératif, qui peut résulter d'une stratégie voulue, conditionne la capacité d'une armée à manœuvrer dans un contexte où le réseau s'étend désormais jusqu'aux échelons tactiques les plus bas.

Les opérations militaires impliquent l'expression d'une stratégie qui s'appuie sur une architecture, des capacités, et un format d'armée. Etablies dans un but de guerre, elles reflètent la combinaison de cet ensemble sur un espace dans un temps donné. Dans ce déploiement, le rôle des réseaux humains et techniques a pris une nouvelle dimension pour établir les conditions d'un engagement favorable.
Comme toujours, la capacité à générer des alliances de circonstances[1] pour appuyer son action apparaît primordiale. En 2003, les États-Unis se sont engagés en Irak en cherchant des alliés. Pour aboutir à la génération de forces, la mise en place de réseaux techniques et humains est nécessaire. Ce besoin n'est pas l'apanage du temps de guerre, et il commence dès le temps de paix. L'enjeu est lié à la collecte et au traitement de l'information utile pour l'opération militaire. Apparaissant sous forme de données et transportée par des supports physiques, l'information est devenue à la fois un moyen et un enjeu. Elle conditionne la conduite de la manœuvre militaire et revêt les caractéristiques d'une arme pouvant affaiblir la volonté de l'adversaire. Elle s'applique sur l'ensemble de la gamme des opérations actuelles.
De la coercition en passant par le maintien de la paix jusqu'à la guerre irrégulière, elle est au centre d'une bataille pour la détection contre la discrétion, et l'interception pour la

[1] Tactique théorique, Colonel Michel Yakovleff, Economica, 2006.

destruction. Chaque adversaire tente, suivant les circonstances, de maîtriser à un moment donné de l'action militaire ces quatre temps. Dans ce cadre, la distanciation relative des champs de bataille actuels génère des élongations importantes dans la transmission des informations au profit des armées. Ce phénomène, décuplé par la constitution d'armées très mobiles capables de s'affranchir de l'espace, induit la maîtrise de la logique de réseaux.
Si la conduite de la guerre introduit les réseaux dans l'action stratégique et opérative, elle introduit également des procédés novateurs qui s'appliquent aux différentes phases de déclenchement d'une opération.

I - La nouveauté des réseaux dans la conduite de la guerre

Source de prospérité et de puissance, la convergence des réseaux humains et techniques donne aux opérations militaires un rythme qui permet la surprise stratégique et tactique.

1.1. Le rôle de l'innovation dans la supériorité stratégique

Si l'innovation est l'occasion de rebattre les cartes et de changer les règles du jeu, elle ne s'anticipe que très difficilement. De plus, dans la guerre, il faut s'assurer avant toute chose des conditions qui la rendent possible dans les opérations. Elle s'exprime autant par des méthodes que des moyens, en donnant une efficacité nouvelle à une manœuvre ou une opération.
Lors de la Première guerre mondiale, un commandant en chef devait posséder des capacités d'artillerie pour mener des offensives efficaces. En 1940, l'aviation[2] en appui des blindés apparaissait comme décisive pour réaliser ce genre d'opérations.
Or, depuis 1945, l'évolution de l'art de la guerre nécessite plus une aptitude à combiner l'ensemble des moyens classiques avec l'aide des réseaux. Cette pratique n'est pas neuve. Les armées romaines et mongoles ont basé leur supériorité sur une capacité à maîtriser leurs mouvements à partir des aspects techniques et humains de leurs réseaux[3].
Cependant, la technologie d'aujourd'hui permet de donner une autre forme aux opérations militaires et concourt à conduire autrement la guerre dans les phases de conception, de planification, de mise en œuvre, et d'exécution. Aussi, les modèles d'armées qui se profilent incluent des capacités de lutte dans le monde des réseaux appelé cyberespace.
La conséquence militaire de cette dynamique implique qu'un effet combiné de la guerre électronique et des systèmes d'information et de communications influe sur la manœuvre d'une armée. L'Armée de l'air et la Marine sont actuellement en pointe dans cette intégration des réseaux dans la conduite de leurs opérations, rendant précieux leurs emplois dans la gestion de crise, l'engagement urgent en protection et intervention.
Les armées de terre et les unités spécifiques agissant stricto-sensu dans le cyberespace commencent à peine à intégrer cette particularité dans leurs modes d'action et leurs procédés d'exécution. Partant du postulat que les concepts existent, les conséquences dans la stratégie et la tactique ouvrent des perspectives nouvelles dans le rythme de la manœuvre interarmes et interarmées. Une armée contrainte par son cadre d'emploi et ses ressources peut s'engager dans cette voie pour frapper vite et fort en usant de ces moyens les plus puissants au moment choisi, tout en privilégiant la manœuvre[4]. Dès lors, les technologies réseaux sont facteurs d'innovation dans l'application de l'action militaire.

[2] Le développement du stuka du Colonel Von Richthofen fut, par exemple, décisive dans l'exploitation de la percée allemande en mai 1940.
[3] L'armée romaine, Catherine Wolf, CNRS, éditions Paris 2012.
[4] Le mythe de la guerre-éclair, la campagne de l'ouest de 1940, Karl-Heinz Frieser, Paris, Belin, 2003.

1.2. L'importance des armées construites en système

Si le maréchal Foch établit trois grands principes qui s'érigent en ligne de conduite pour tout commandant en chef[5], l'analyse *a posteriori* des batailles historiques montre que l'application consciente de la liberté d'action, la concentration des efforts, l'économie des moyens, conduit à la victoire ou à la défaite en fonction des circonstances.

Ce trait apparaît dans son aspect le plus aigu dans les guerres de coalition et celles où le rapport de force est défavorable à une des parties[6]. Ces caractéristiques démontrent comment une armée érigée en système associée à la qualité manœuvrière des troupes et des commandants en chef peut inverser une situation défavorable. Même si une armée disposant de gros effectif possède une capacité de régénération plus importante dans le temps, elle peut être battue par un adversaire plus intelligent et manœuvrier. Et comme les ordres de batailles sont assujettis à la nature des armes, la construction des unités reflètent également la létalité des technologies du moment. Aussi, la lutte pour combler le décalage entre les possibilités qu'offrent la technique et son intégration dans les armées crée toujours des comportements archaïques, phénomène qui se révèle en partie dans la guerre.

Les technologies réseaux adaptées à la stratégie et à la tactique génèrent un décalage avec l'acceptation sociologique des nouveaux concepts qu'elles engendrent. Elles supposent une maîtrise de la dynamique produite par les effets de la cybernétique dans chaque armée à travers chaque élément technique ajoutés aux tâches humaines. En encourageant le fonctionnement intégré, la cybernétique formate un système d'armée exigeant en méthode et en organisation. La manière d'intégrer et de comprendre cette innovation liée aux réseaux constitue la clé d'une conduite des opérations dans un style nouveau.

1.3. L'adaptation des réseaux à la guerre

L'armement ne détermine pas l'issue des combats, il conditionne leurs formes et modifie les combinaisons entre les armes et les armées. C'est pourquoi, l'art de la guerre doit se réinventer aux moments où la technologie redistribue les facteurs contribuant à la victoire. D'autant que, les facteurs de supériorité opérationnelle pour un engagement urgent en protection et en intervention impliquent des conditions préalables. La capacité à créer des réseaux sous un court préavis à partir d'une forte coordination fixe le niveau de puissance de l'engagement. Celle-ci est transverse car elle touche à la logistique, aux appuis, et la mêlée. Elle fait également face aux attaques adverses qui tentent de limiter, détruire ou perturber ce déploiement.

Les réseaux engendrent donc des conséquences profondes dans les systèmes politiques et sociaux. Ils modifient les organisations dans leurs fonctionnements et leurs capacités d'actions. Ils renforcent notamment la capacité à surprendre un adversaire en offrant à la disposition du chef militaire des possibilités d'actions brutales sur de longues distances[7]. La démonstration faite par l'armée américaine lors de la Première guerre du Golfe[8] a fixé cette nouvelle condition pour toute opération.

---

[5] Les principes de la guerre, Maréchal Foch, Economica, 2007. Ces principes sont la liberté d'action, la concentration des efforts, l'économie des moyens.

[6] Les exemples historiques sont multiples. On peut citer les guerres de l'Empire napoléonien et les conflits israélo-arabes entre 1948 et 1973

[7] Conduite sous la forme de cyber-opérations dans les réseaux.

[8] En particulier pour l'arme aérienne.

C'est pourquoi, l'adaptation des réseaux à la guerre consiste à remporter dès le temps de paix la bataille de l'information[9] dans la définition la plus large attribuée au cyberespace[10]. Une opération menée sans maîtrise des réseaux est condamnée à subir le rythme de son adversaire. La base de cette puissance vient d'une économie numérique puissante appuyée par un système étatique lui-même organisé en réseau[11].
Cet aspect modifie les organisations militaires qui, pour survivre, doivent s'adapter à ce contexte. S'il existe deux possibilités parant aux défauts d'une organisation - la coordination des individus à travers des réseaux humains, et la compétence propre des personnalités -, ce mouvement pousse les chefs militaires à constamment transformer leurs forces en système. Dans ce cadre, si les principes de Foch restent pertinents, les réseaux en suscitent de nouveaux dans les procédés de combat.

II - De nouveaux procédés de combat

Trois procédés peuvent être ainsi identifiés : la poly-centralité, la dispersion, la protection. Ces derniers n'ont pas vocation à chercher la distance mais plutôt une convergence des efforts. Le but étant d'appliquer la violence de guerre dans un style fulgurant sans que le positionnement initial des unités ne laisse présager d'un mouvement offensif.

2.1. Poly-centralité

La poly-centralité permet de créer des nœuds réseaux pouvant étendre l'élongation des opérations jusqu'à des milliers de kilomètres. Ils sont associés aux dorsales réseaux maillant les territoires, et aux systèmes satellitaires pour les nations les plus riches.
Cela signifie que la puissance militaire d'un pays s'appuie sur une aptitude à mailler la géographie physique des lieux en routes et réseaux de communications. Les opérateurs nationaux ainsi qu'une bonne densité de data-centers fournissent le socle de cette poly-centralité. En captant de la donnée sur un lieu à un moment précis à partir d'usines numériques, les nations produisent de la valeur ajoutée pour leurs actions propres à la défense de leurs intérêts. Lors d'une opération, ce système du temps de paix concourt à faciliter les changements rapides de position des forces sur un terrain donné en s'appuyant sur une architecture de systèmes d'information et de communications modulable.
De même, la poly-centralité favorise l'expression de la puissance de feu dans un style nouveau. Comme le rapport puissance de feu et nombre d'unités ne cessent de croître avec la technologie, le champ de bataille devient un vide menaçant dans lequel une attaque surgit et disparaît en fonction des objectifs. Une armée, qui ne serait pas dotée de facteurs de poly-centralité, ne pourrait pas s'engager dans un combat mobile sans risquer d'être détruite avant son mouvement[12]. Ainsi, tout ce qui transporte l'information multiplie les chances d'une bonne coordination sur des espaces complexes[13] à des niveaux supérieurs de combinaison.

[9] Guerre et manœuvre, sous la direction de Christian Malis, Economica, fondation Saint-Cyr, 2009.
[10] Tout ce qui transite sous forme de données.
[11] La théorie de l'information, Aurélien Bellanger, Gallimard, 2012.
[12] L'armée irakienne lors de la guerre du golfe de 1991
[13] Le développement des drones de combat aérien et terrestre permettent également de les transformer en antennes relais mobiles pour les forces armées.

2.2. Dispersion

La dispersion devient également un procédé. Plus une opération militaire dispose d'une force capable de créer du réseau, plus les unités peuvent s'éloigner les unes des autres. Cette tendance permet d'entretenir le brouillard de la guerre pour l'ennemi[14]. Il ne perçoit pas l'effort principal et les possibilités de combinaison susceptibles de s'abattre sur lui. Les armées allemandes ont pratiqué ce principe au début de la campagne de 1940 empêchant le commandement français de connaître l'effort principal. À l'inverse, une armée ne pouvant pas se disperser cherchera en phase initiale à se concentrer, et sera d'autant plus vulnérable aux frappes lors de ces manœuvres[15]. Dès lors, une double lutte s'engage entre la détection/discrétion et l'interception/destruction. Ce combat s'appuie sur des systèmes d'information et de communications qui sont utilisés par des entités autres que les traditionnels postes de commandement. Ainsi, un soldat, tout comme un armement, peut constituer un capteur ou un diffuseur.

D'autres problématiques émergent du procédé de dispersion. Il dilue les responsabilités et les opportunités tactiques si les réseaux ne sont pas construits dans une logique hiérarchisée à partir d'une discipline d'emploi au niveau des États-majors et des unités. L'isolement propre à la dispersion implique des qualités de jugement et de conduite supérieures. L'autonomie qui doit s'y manifester et la vision du moment déterminent le résultat de la manœuvre. Ce fait apparaît dans le processus de décision. Voir dans la dispersion une capacité de frappe par rapport à une opportunité tactique ou stratégique suppose un raisonnement intégrant des informations éparses et partielles des unités éloignées, dans une équation où les réseaux réduisent ou élargissent les combinaisons pour les chefs.

2.3. Protection

La protection constitue le dernier procédé de combat. Il permet de conserver la liberté d'action des États et de leurs forces armées vis-à-vis d'autres pays, mais également face à des groupes non-étatiques disposant d'une puissance numérique[16].

Pour imposer une asphyxie à son adversaire avant même qu'il ne puisse se mettre en ordre de marche, le tempo induit des plans de continuité et de reprise d'activité des réseaux militaires et étatiques. Ils répondent aux possibles des cyber-attaques stratégiques et tactiques.

Comme chaque création de territoire génère une lutte pour sa possession, le cyberespace n'échappe pas à ce phénomène. Il reproduit les tensions internationales sous d'autres formes. Autrement dit, un adversaire cherchera à agir dans le champ numérique à des niveaux plus ou moins techniques pour briser le rythme de l'opération. Le but de ces plans est de limiter les effets d'une offensive sur les réseaux nationaux.

Perçu autant comme un lieu d'échanges et d'affrontement[17], le cyberespace, à la différence des espaces physiques, n'est pas contrôlable car les interconnexions sont telles qu'elles laissent aux États deux possibilités de contrôle. Soit ils opèrent un black-out des réseaux, ce qui semble peu réaliste si l'on considère le rôle que les réseaux jouent dans les économies. Soit ils tentent de filtrer, de réglementer et de formaliser les réseaux ce qui n'est pas aisé à réaliser, mêmes par les plus grandes cyber-puissances.

---

[14]Pour faire face à cette problématique lors de la Première guerre du Golfe, les Irakiens déclenchaient des feux volontaires autour de leurs blindés pour éviter d'être frappés par les frappes aériennes d'opportunité de la coalition.

[15]L'opération Tempête du désert de 1991 montre comment l'Air Force a quadrillé le terrain obligeant les forces irakiennes à s'enterrer et se disperser.

[16]Par exemple le Hezbollah, Anonymous, les Blacks blocks.

[17] Cyber stratégie l'art de la guerre numérique, Bertrand Boyer, Nuvis, 2012.

La protection vise donc deux adversaires : les États et les organisations non-étatiques. Dans les deux cas, l'action militaire est confrontée aux caractéristiques quantiques des mouvements. Elles engendrent des changements brutaux d'état de situation liés notamment au nombre de connexions associées à leurs portées. Ce terrain mouvant conduit à des vulnérabilités mises à profit par des attaquants. L'expérimentation du drone X47B reflète en partie cette problématique. En se dotant d'un drone capable de se catapulter depuis un porte-avion, la *Navy* dispose d'une plus grande élongation pour frapper des objectifs en cas d'attaque chinoise sur Taïwan, tout en plaçant son groupe aéro-naval hors de portée. Sur le plan tactique, cette notion de protection implique la défense de l'intégrité physique des supports et des points d'accès des réseaux nationaux.
Face à des organisations non étatiques, les réseaux favorisent la dissidence, l'émergence de réseaux parallèles et des attaques mélangeant le style direct et indirect. La protection implique de lutter contre leurs actions offensives en adoptant les mêmes méthodes, tout en se plaçant au même niveau d'engagement. Elles concernent autant la stratégie que la conduite tactique. Dans la stratégie, elles déstabilisent les États. Lors de l'embuscade Uzbeen, les talibans ont mené une campagne médiatique fortement relayée par les réseaux. Ils ont amenés les politiques à se poser la question de la pertinence de l'engagement français en Afghanistan.
À l'inverse, les forces kenyanes ont largement utilisé Twitter pour communiquer en temps réel sur la prise d'otages de Nairobi en 2013, tout en évitant que les médias traditionnels prennent l'initiative de l'information. Ce constat d'ensemble sur les procédés de combat liés aux réseaux transforme les opérations qui apparaissent comme un moyen d'appliquer une stratégie[18] originale.

III - Adapter les phases stratégiques

Une opération militaire se décompose en plusieurs phases : la conception, la planification et l'exécution : chacune nécessite la prise en compte d'une approche par les réseaux[19].

3.1. La conception

La conception d'une opération relève d'une combinaison de moyens disponibles orientés vers un objectif, dans le cadre d'un environnement contraint. Elle s'inspire d'un plan de guerre qui se transforme en plan d'opérations, et conduit à la constitution et la projection d'une force dans des milieux lointains et contraints.
Les plans visent à maîtriser la création d'une zone autonome temporaire qui se structure autour de systèmes de communication et d'information. La force déployée se structure sur ce dispositif en permettant la combinaison des armes. En déployant une gamme diversifiée de satellites militaires lors de la Première guerre du Golfe, les Américains disposaient d'une liberté d'action dans l'emploi de l'arme aérienne dans une coalition élargie à plusieurs pays.
Remarquons ici deux dimensions à prendre en compte pour la conception d'une opération. Tout d'abord, les réseaux permettent un éclatement géographique des alliances avec un resserrement de l'action géopolitique. Comme un État ne peut pas s'opposer à un autre sans avoir au préalable constitué une communauté d'intérêts, des stratégies en réseaux originales sont établies pour établir des coalitions. Des pays très éloignés peuvent se retrouver autour d'intérêts communs par rapport à une situation particulière. Ce principe prévalait déjà dans le

[18]Comme par exemple les cyber-attaques menées contre l'Iran pour ralentir son programme nucléaire.
[19] La guerre en réseau au XXI siècle, Jean Pierre Maulny, éditions du Félin, 2006.

passé, que ce soit par l'ouverture et le renforcement des routes commerciales ou par les technologies du télégraphe et de la radio. Aujourd'hui, cette tendance se traduit par un rapprochement plus étroit entre les parties, ce qui permet une plus grande réversibilité dans le temps. Ensuite, aucune planification ne peut se cantonner aux problématiques simplement militaires, puisqu'elle doit inclure systématiquement la dimension médiatique sans perdre de vue les objectifs politiques.

3.2. Planification

La planification consiste à définir les étapes nécessaires pour atteindre les objectifs de guerre. Elle vise à articuler une force rendue cohérente par une « bulle réseau » afin de permettre l'engagement autonome ou combiné d'une armée.
Des réseaux nationaux maîtrisés de bout en bout confèrent de la puissance à l'opération. Plus une nation est capable de conjuguer une forte élongation à une vitesse de transmissions de données nécessaires à la conduite des unités, plus ses armées sont capables de se concentrer, de se disperser puis de se recombiner sur de très courts préavis, et sur des distances plus importantes. De plus, La perspective nouvelle donnée par le cyberespace ajoute une autre dimension à ce principe en permettant l'usage de cyber-opérations dans les réseaux civils et militaires adverses[20].

En effet, le développement des terminaux mobiles comme les *smartphones*, les tablettes et les ordinateurs traduisent l'emprise de la problématique des réseaux dans les opérations. Ainsi, le corps des *Marines* intègre le cyberespace dans ses actions de combat, et au sein des états-majors, des cellules de guerre électronique agissent contre les réseaux adverses sur le théâtre d'opération mais aussi contre les infrastructures du pays ennemi[21].
De fait, les opérations militaires s'inscrivent dans une logique de flux qu'induit la prégnance des réseaux, le commandant devant maintenant constamment considérer dans son action les champs de la détection, de la discrétion, de l'interception, et de la destruction.
Cette logique de réseau ne place pas les chefs en retrait, mais au contraire, elle nécessite un commandement de l'avant dans lequel le commandant se place au centre d'un nœud d'informations. Celui-ci peut être temporaire tout en se révélant décisif pour l'action de guerre. De fait, le chef oriente le mouvement de ses unités, et la saisie de l'instant décisif que sentent la plupart des grands chefs militaires devient alors possible. Pour atteindre ce but, le réseau se place comme un moyen de retrouver une emprise sur ses unités face aux distances. Il densifie la propension des unités à pouvoir échanger et communiquer en se basant sur les initiatives des échelons subordonnés.
De ce fait, les réseaux suggèrent de penser les opérations militaires d'aujourd'hui selon la capacité d'élongation plutôt que la concentration des moyens. En maintenant des liens lointains sans rupture des échanges, une armée peut ensuite se concentrer selon les besoins.
Cette particularité se renforce dans un contexte de militarisation du cyberespace où les opérations militaires peuvent s'engager directement à travers les réseaux par des moyens non classiques. Elle implique l'émergence de nouveaux types de soldats comme l'ont été les artilleurs, les aviateurs, les sous-mariniers. Et elle suggère la compréhension et la cartographie des infrastructures de télécommunications à travers un atlas de géographie numérique des fermes de données (*data centers*) et d'autres nœuds de transmissions amis et ennemis. Les conséquences sur la conduite des opérations nécessitent la sanctuarisation de l'environnement

[20] « Guerre intégrée électronique et en réseau », Major Général Dai Qingnim, China military science, 2007.
[21] Chinese and American network warfare, Timothy L.Thomas, 2005.

électromagnétique s'appuyant sur le renseignement « cyber »[22]. Une faiblesse dans la maîtrise de cette phase empêche toute exécution d'opérations d'envergure.

3.3. Exécution

Le procédé d'exécution intègre la gestion et le traitement de l'information dans les opérations. Ces deux processus impliquent davantage de coordination et de discipline formelle dans le transfert d'informations[23], et modifient également la forme des organisations militaires.
De nos jours, les armées mondiales effectuent des choix différents en matière d'échelon tactique de référence. Certaines conservent la division quand d'autres s'orientent vers la notion de groupement d'armes concentrées au sein d'unités resserrées. L'intégration des réseaux confère au groupement une mobilité supérieure à celui d'un échelon de division classique, ceci en augmentant le ratio vitesse/puissance dans la manœuvre.
Cet effet se matérialise au niveau des unités élémentaires par l'ajout d'un adjoint gérant les flux d'informations au niveau du commandant de compagnie. *De facto*, ce besoin s'élargit jusqu'au niveau du théâtre d'opération où les adjoints réseaux ont la responsabilité des bases de données militaires appartenant aux intérêts vitaux des pays. Dès lors, dans la manœuvre, les fournisseurs d'infrastructures techniques deviennent des acteurs stratégiques car ils déterminent les routes de l'information avec les univers physique et numérique déterminant en partie le cadre de l'opération militaire.
Le Général Ferrié utilisa lors de la Première Guerre mondiale un poste français maquillé en centre allemand qui transmettait aux Zeppelins des rectifications de route : celles-ci amenaient les dirigeables au-dessus des camps d'aviation et des batteries françaises.
Qui plus est, les infrastructures techniques sont désormais commutées en fonction de l'intensité du trafic et des priorités. L'artère principale, communément appelé le *Backbone*, relie les centres majeurs où les noms des domaines sont vérifiés, les adresses authentifiées, les communications redistribuées.
La généralisation des fermes de données associées à des solutions d'informatique en nuage se transforme en cibles stratégiques pour l'arme aérienne et les missiles.
Ensuite, les réseaux peuvent faire l'objet de manœuvre de déception en renforçant le traditionnel brouillard de guerre par l'altération, la paralysie ou la destruction des informations. Les opérations militaires peuvent alors s'appuyer sur des actions numériques. Comme le démontre la troisième loi de Newton qui veut que chaque action entraîne une réaction égale et opposée, elles engendrent des cyber-opérations dans le cyberespace à partir des principes tactiques de la guerre classique. Elles recherchent la paralysie[24], le renseignement[25], la destruction. En ciblant des objectifs précis intégrant des faiblesses systèmes non connues de l'adversaire, avec leur effet multiplié par le réseau dans lequel elles doivent manœuvrer, les cyber-armes disposent d'un potentiel de destruction. En 2012 par exemple, le virus Shamoon a infecté la compagnie pétrolière saoudienne Aramco et provoqué la destruction de 35 000 ordinateurs.

Cet état rapproche très étroitement la conception, la planification et la conduite des opérations militaires. Si ce phénomène existe depuis l'introduction de la radio dans les opérations militaires, il s'accélère avec le maillage renforcé introduit par le cyberespace. Pour la première fois lors de la Première Guerre mondiale, une armée disposait de la TSF pour

[22] Il est plus général que le renseignement d'origine électromagnétique
[23] Psychologie de la bataille, Karpov et Jean-François Phélizon, Economica, 2004.
[24] Saturation de la bande passante
[25] Opération Newcaster, Thierry Berthier

conduire et intercepter les communications adverses. La Seconde Guerre mondiale a renforcé cette tendance par l'adjonction de systèmes radio dans les unités.

Aujourd'hui, les retours des expériences de guerre brouillent ce phasage par l'effet fulgurant des réseaux. La multiplication des capteurs et l'arrivée de l'Internet dans la guerre change l'approche stratégie et tactique d'une opération militaire.

Conclusion

La convergence de la stratégie et des réseaux dans les opérations militaires relève de la cyber-géopolitique. Une opération n'aura de valeur qu'à la condition de maîtriser, à un moment donné, le cyberespace dans sa définition la plus large. De plus, les armées ne se déplacent plus uniquement sur leurs territoires ou ceux de leurs voisins proches, elles s'engagent dans des interventions qui nécessitent de combiner autrement la force.
Dans ce cadre, l'économie numérique devient un enjeu de souveraineté. Son développement génère de la puissance militaire à travers la densification des réseaux, et leur utilisation.
Le but consiste à maintenir un contrôle relatif du territoire physique par la maîtrise de son espace numérique. Pour cela, mieux vaut raisonner en logique de points d'entrée plutôt qu'en logique de défense de frontière.
Comprenant ce principe, la Chine comme Israël constituent des exemples uniques de stratégies originales civile et militaire, bâtissant une souveraineté numérique qui s'appuie dans le cas chinois sur des normes propres et sur un volume d'internautes dépassant ceux des autres États, avec pour conséquence que l'ouverture programmée de ses réseaux au reste du monde ferait de ce pays la première puissance numérique au monde.