.

« LA RESILIENCE *HORS LIMITES* DES GROUPES ARMES»

DANS QUELLE MESURE LES TRANSFORMATIONS NUMERIQUES DE LA SOCIETE ET LES DERNIERES INNOVATIONS TECHNOLOGIQUES PERMETTENT AUX PETITS GROUPES ARMES D'ETRE PLUS RESILIENTS QUE DE GRANDES ARMEES ETATIQUES ?

Tuteur :

LCL ENTRAYGUES Olivier

Auteur :

CBA Jean-François CAVERNE

RESUME

La transformation numérique de la société et la globalisation des technologies récentes génèrent et alimentent un nouvel ordre sur l'échiquier planétaire. Des acteurs insurrectionnels (terroristes, groupes armés paramilitaires), autrefois voués à disparaître de par leur taille insignifiante, trouvent dans la large diffusion et démocratisation des technologies d'intérêt militaire une source de résilience considérable. Cela entraîne un opportunisme technologique auprès d'acteurs imprévisibles.

Malgré les frappes et les dommages causés par des grandes armées étatiques présentées technologiquement et opérationnellement supérieures, la capacité d'acteurs de second ordre à se régénérer, se recomposer et à maintenir leur développement amène à étudier qui sont ces belligérants, et dans quelle mesure les transformations numériques de la société et les dernières innovations technologiques leurs permettent d'être plus résilients que de grandes armées étatiques.

Si les dernières avancées numériques et techniques de la société occidentale constituent un vecteur incontournable de la supériorité technologique et opérationnelle de grandes armées étatiques, il n'en demeure pas moins vrai que le « pouvoir nivelant » de ces technologies tend à rendre ponctuellement des adversaires asymétriques sinon invulnérables, du moins capables de neutraliser l'avantage du fort. Leur résilience devient « hors-limites ».

Dans un premier temps, la compréhension des « ressorts technologiques actuels » à la portée des petits groupes armés permet de mesurer leur influence sur le renforcement de leur résilience. Ensuite, pour saisir en quoi la résilience obtenue par de tels belligérants peut dérouter de grandes armées étatiques, il est nécessaire de conceptualiser les piliers de cette résilience. L'identification de 4 piliers distincts (piliers organisationnel, informationnel, opérationnel et structurel) permet d'évaluer dans quelle mesure les nouvelles technologies cimentent et fortifient directement ces piliers. Enfin, il ne faut pas oublier que ces technologies peuvent également constituer un « atout trompeur » dans la résilience même des armées de grande puissance, et de créer une inversion de la résilience attendue.

ABSTRACT

The digital transformation of society and the globalization of recent technologies are generating and fueling a new order on the international chessboard. Insurgent actors (terrorists, paramilitary armed groups), once destined to disappear because of their insignificant size, find in the wide diffusion and democratization of technologies of military interest a source of considerable resilience. This leads to technological opportunism with unpredictable actors.

Despite the strikes and damage caused by large state armies presented technologically and operationally superior, the ability of second-rate actors to regenerate, recompose and maintain their development leads us to study who these belligerents are, and to what extent the digital transformations of society and the latest technological innovations allow them to be more resilient than large state armies.

While the latest technological and numerical advances in Western society are a key factor in the technological and operational superiority of large state armies, the fact remains that the "leveling power" of these technologies tends to make punctually asymmetric opponents if not invulnerable, at least able to neutralize the advantage of the strong. Their resilience becomes "out of bounds".

As a first step, understanding the "current technological drivers" within the reach of small armed groups makes it possible to measure their influence on strengthening their resilience. Then, to understand how the resilience achieved by such belligerents can confuse large state forces, it is necessary to conceptualize the pillars of this resilience. The identification of 4 distinct pillars (organizational, informational, operational and structural pillars) makes it possible to evaluate to what extent new technologies cement and fortify these pillars directly. Finally, it should not be forgotten that these technologies can also be a "misleading asset" in the resilience of high-powered armies, and create a reversal of expected resilience.

Introduction 1

1. L'intégration numérique et technologique « hors limites » de la société du 21ième siècle 3

1.1. Un nouvel ordre numérique et technologique 3

1.2. Une nouvelle donne entre le monde civil et militaire 5

2. La résilience « hors limites » des groupes armés modernes 8

2.1. Les « techno-belligérants » du 21ème siècle 8

2.2. Conceptualisation de la résilience des groupes armés 11

2.3. Les piliers de la résilience des groupes armés 12

2.4. Les piliers de résilience de l'approche défensive 13

2.5. Les piliers de résilience de l'approche proactive 14

2.6. Le drone, « le meilleur ami du terroriste » 16

2.7. « Le cyber, empire de l'asymétrie » 20

2.8. Les outils de géolocalisation, compagnons indispensables aux groupes armés 30

2.9. L'impression 3D 32

3. « L'atout trompeur » des technologies pour les grandes armées étatiques au 21ième siècle 33

3.1. La porte du chaos 33

3.2. Des géants aux pieds d'argile 34

3.3. Retour de flammes 36

Conclusion 40

Annexe 41

Sources et bibliographie 42

Dans le chapitre « *Les menaces et les risques amplifiés par la mondialisation* »[1], le dernier livre blanc sur la défense et la sécurité nationale de 2013 identifie la dynamique de démocratisation et globalisation des dernières innovations technologiques qui bouleverse notre société dans toutes ses composantes, jusqu'à remettre en cause la dialectique du « fort » au « faible » dans le champ de bataille moderne. Dans son ouvrage *Cybertactique Conduire la guerre numérique*, le lieutenant-colonel Bertrand Boyer illustre les combats du quotidien pour les grandes armées étatiques à « *une nouvelle forme de petite guerre, usure de la défense, multiplicité des formes d'attaques. C'est le combat du lion contre la mouche* »[2]. Si la stratégie de contournement dans les conflits asymétriques a toujours été recherché par le faible, il est troublant aujourd'hui de constater l'impuissance du « fort » à neutraliser efficacement le « faible » malgré sa suprématie technologique régulièrement mise en avant. Accessible au plus grand nombre, les technologies modernes commercialement disponibles confèrent entre les mains de belligérants, jusqu'à alors isolés, une résilience inattendue par leurs adversaires plus puissants. Ce caractère dual et paradoxal des technologies de pointe « low cost » apparaît préoccupant pour la sécurité des nations et de leurs soldats confrontés aux acteurs asymétriques du 21ème siècle.

A l'aune de ce constat, dans quelle mesure les transformations numériques de la société et les dernières innovations technologiques permettent aux petits groupes armés d'être plus résilients que de grandes armées étatiques ?

Accessible commercialement sans barrières réglementaires, les dernières innovations technologiques « bon marché » aux capacités égalisatrices, englobent ici les technologies duales que sont les drones (gamme civile), la téléphonie cellulaire, le GPS et l'impression 3D ; mais également les outils associés à la transformation numérique de notre société que sont les réseaux sociaux, les applications de messagerie sécurisée et les technologies du monde Internet.

Si les dernières avancées numériques et techniques de la société occidentale constituent un vecteur incontournable de la supériorité technologique et opérationnelle de grandes armées étatiques, il n'en demeure pas moins vrai que le « pouvoir nivelant » de ces technologies tend à rendre ponctuellement des adversaires asymétriques sinon invulnérables, du moins capables de neutraliser l'avantage du fort. Leur résilience devient « *hors-limites* ».

1 *Livre blanc sur la défense et la sécurité nationale de 2013*
2 Bertrand BOYER, *Cybertactique Conduire la guerre numérique*, Nuvis, p 166

Pour mesurer l'influence des innovations technologiques sur le renforcement de la résilience des petits groupes armés, il faut en premier lieu découvrir les ressorts technologiques actuels à leur portée et la « technosphère » associée au potentiel considérable. Ensuite, pour comprendre en quoi la résilience obtenue par de tels belligérants peut dérouter de grandes armées étatiques, il faut appréhender les piliers de cette résilience et l'apport des différentes technologies dans le maintien de ces piliers. Enfin, il convient de discerner et de saisir dans quelle mesure ces technologies peuvent constituer un « atout trompeur » dans la résilience des armées de grande puissance.

* *

*

1. L'intégration numérique et technologique « hors limites »[3] de la société du 21ième siècle

Pour comprendre comment les transformations numériques de la société et les dernières innovations technologiques peuvent permettre aux petits groupes armés d'être plus résilients que de grandes armées étatiques, il faut dans un premier temps prendre l'ampleur de l'explosion numérique et technologique et de ses répercussions à laquelle la société assiste depuis la fin des années 90.

1.1. Un nouvel ordre numérique et technologique

Une dynamique expansionniste dans le domaine du cyber et des technologies innovantes impose un potentiel et un rythme hors du commun à la société du 21ème siècle. Cette vague numérique et technologique entraîne des révolutions d'usage dans nos sociétés, dans les grandes armées étatiques et également chez des acteurs jusqu'alors imprévisibles comme les groupes pratiquants une insurrection armée (terroristes, groupes armés paramilitaires). Un changement de paradigme que les colonels chinois Qiao Liang et Wang Xiandsui avait annoncé au début des années 2000 : « *Tout change. Explosion technologique, remplacement de l'élargissement de la notion de sécurité, ajustement des objectifs stratégiques, brouillage des frontières du champ de bataille, extension de l'amplitude des moyens non militaires et des personnels non militaires impliqués dans la guerre...* »[4].

La transformation numérique

Au milieu des années 90, la numérisation a désigné les procédés et techniques de conversion des contenus véhiculés sur supports analogiques en données numériques (éléments binaires : 0 ou 1) exploitables par les technologies de l'information et de la communication. Cette dématérialisation a touché toute la société dont le monde militaire pour lequel ces technologies ont provoqué un véritable tsunami informationnel. De manière croissante et irréversible, ces outils se sont imposés dans la société contemporaine et dans l'espace de bataille moderne. Tout le monde est aujourd'hui globalement connecté à Internet, en permanence. Chacun peut recevoir et transmettre de l'information en temps réel depuis n'importe quel lieu. Ce bouleversement spatio-temporel est d'autant plus stupéfiant qu'il a permis l'entrée d'acteurs, individus ou groupes, avec de grandes capacités d'actions ou d'influence où personne ne les attendait.

3 Expression issue de l'ouvrage *La guerre hors limites* des colonels chinois Qiao Liang et Wang Xiandsui, Rivages poche.
4 Qiao Liang, Wang Xiandsui, *op cit.*, page 177.

Depuis l'avènement de l'ordinateur, les mutations dans le domaine numérique sont considérables au point de parler en ce début de 21ième siècle de transformation numérique (ou digitale). A l'image de la révolution industrielle qui a profondément modifié la société du 19ème siècle, la transformation numérique bouleverse notre société actuelle. Cette transformation existe depuis l'essor d'Internet, mais le rythme effréné des innovations technologiques de ces dernières années lui donne une dimension considérable. Aujourd'hui, elle désigne le processus qui permet à tous les acteurs de notre société d'intégrer toutes les technologies numériques disponibles au sein de leurs activités pour améliorer leur efficacité. Elle vise à compléter le « faire mieux » des NTIC[5] avec le « faire différemment » grâce aux toutes dernières innovations technologiques : développement du Cloud, de l'Internet des objets, du « smart data », de la santé connectée, ou bien encore de la réalité virtuelle…

Cependant cette transformation va bien au-delà des dizaines de milliards d'objets connectés dont les médias et entreprises nous annoncent l'avènement. Cela est réducteur de la cantonner uniquement à la révolution d'Internet et de ses outils technologiques. Elle passe aussi par le facteur humain, avec sa façon de penser qui évolue simultanément. Bercée dans le monde des nouvelles technologies, les générations actuelles et futures embrassent un nouvel espace de vie, un nouveau milieu où l'imagination n'a plus de limites : le cyberespace. La définition du Concept D'Emploi des Forces le désigne comme « *le réseau planétaire qui relie virtuellement les activités humaines grâce à l'interconnexion des ordinateurs et permet la circulation et l'échange rapides d'informations* »[6].

Ce nouvel espace de manœuvre aussi englobant que virtuel apparaît comme sans frontières, anonyme, source de libertés, d'échanges et de communication, « *mais également un espace dangereux et nébuleux dans lequel des comportements réprimés en société peuvent s'exprimer sans répression* »[7]. En effet, le cyberespace permet à des idéologies de se diffuser comme une traînée de poudre, et il démocratise et développe la production d'information pour renseigner, coordonner, organiser, rassembler, guider,…

5 Nouvelles Technologies de l'Information de la Communication.
6 Centre interarmées de concepts, de doctrines et d'expérimentations, *Concept d'emploi des forces (CEF)*, CIA –0, Concept interarmées N° 004/DEF/CICDE/NP du 11 janvier 2010, page 26.
7 Alix Desforges , *Les représentations du cyberespace : un outil géopolitique*, Hérodote, Cyberespace : enjeux géopolitiques, 2014/1 (n° 152-153).

La société technologique 4.0

« *Le terme 4.0 est explicite : une quatrième révolution industrielle est en marche, comparable à l'introduction de la machine à vapeur, de l'électricité ou de l'électronique* »[8]. Les changements sociétaux « *s'opèrent petit à petit, mais le temps entre l'arrivée d'une technologie et son adoption dans les usages courants est de plus en plus court. Lorsqu'une technologie apparaît, elle accélère la précédente et s'y associe, rendant celle-ci plus simple et plus rapide d'utilisation* »[9]. Depuis vingt ans, de multiples petites révolutions sont donc apparues dans la société grâce à l'émergence et la diffusion générale d'innovations technologiques jusqu'alors réservés à une minorité : drones, smartphones, téléphonie satellitaire, ordinateurs et supports numériques (clé USB et disques durs portables), géolocalisation (GPS), imprimantes 3D, …

Cette société 4.0 est celle qui bouleverse chaque jour un peu plus l'expérience humaine en offrant une source exponentielle d'opportunités et de nouveaux défis. Les dernières innovations deviennent les prolongements des individus, et ont un impact direct sur notre société. Elles sont autant d'outils avec lesquels on peut repenser fortement les compétences des individus, leurs capacités et potentiel d'action, et tous les environnements et situations où l'être humain évolue. Cette ère technologique ancre définitivement dans le passé les techniques rigides et réservées à une élite. Elle restructure en profondeur la société contemporaine par une accélération et une contraction technologique.

1.2. Une nouvelle donne entre le monde civil et militaire

Si l'explosion numérique et technologique de ce début du 21 siècle est majeure, la répercussion sur la société contemporaine est hors du commun au point d'évoquer un changement de paradigme. Une révolution conceptuelle qui se base sur une inversion de la maîtrise des technologies d'intérêt militaire. En effet, la recherche privée prend la distance sur la recherche militaire sur les technologies de pointe. Traditionnellement la suprématie des grandes armées étatiques occidentales était dynamisée stratégiquement par une recherche militaire prééminente sur la société. Et cette inversion est double avec la fin du monopole sur l'accès à ces technologies militaires de pointe.

8 Dorothée Kohler, Jean-Daniel Weisz, *La France doit s'inspirer du projet « Industrie 4.0 » allemand*, Le Monde, 14/11/2014.
9 http://www.mbadmb.com/2016/12/11/societe-4-0/, consulté le 16/01/2016.

La large diffusion et démocratisation de ces technologies est à la source du triomphe de l'opportunisme technologique et au nivellement de puissance entre de nombreux acteurs de tout type à l'échelle planétaire.

Une recherche militaire poussée en dehors de certains domaines technologiques

Internet, drones, GPS, cryptographie … les armées des grandes puissances, autrefois initiatrices de nombreuses révolutions technologiques, n'ont plus le monopole de l'innovation majeure. Plusieurs experts scientifiques et du monde de la défense font part de leurs inquiétudes dans la dernière revue stratégique française parue en 2017 : « *Historiquement, les ruptures majeures en matière d'armement ont été le fruit de financements à finalité militaire* »[10]. Ces dernières, poussées hors de certains domaines technologiques par des acteurs civils de plus en plus actifs qui font « *émerger un nombre croissant de technologies d'intérêt militaire* »[11].

Big data, impression 3D, intelligence artificielle, objets connectés… Les technologies de pointe ne sont plus donc réservées à un club réduit d'acteurs étatiques et de leur recherche militaire. Elles sont plus que jamais accessibles. De plus avec Internet, il y a une dynamique générale de diffusion de ces techniques. Les grandes nations n'ont plus la capacité de garder la maîtrise des technologies de pointe qui étaient autrefois les piliers de leur suprématie. Ainsi, le drone est passé du domaine militaire au domaine civil en quelques années seulement. Comme le constatent les colonels chinois Qiao Liang et Wang Xiandsui, « *actuellement, il est beaucoup plus difficile de conserver le monopole d'une technique que d'en inventer une* »[12].

Démocratisation des technologies d'intérêt militaire et nivellement de puissance

Largement diffusée, les nouvelles technologies d'intérêt militaire alimentent un opportunisme technologique qui conduit à un nivellement de puissance. Des acteurs jusqu'alors insignifiants accèdent à des technologies au rapport « coût / efficacité » capable de déstabiliser, d'influencer un ordre local, voire régional et au-delà.

10 Revue stratégique de défense et de sécurité nationale 2017, page 33.
11 *Id.*
12 Qiao Liang, Wang Xiandsui, *op cit.* , page 167-168.

Certains « *Etats de taille intermédiaire, mais aussi des individus isolés ou des groupes* »[13] accèdent à des « *capacités jusqu'ici maîtrisées par un nombre restreint d'États* »[14], ce qui « *tend à niveler les rapports de force militaires* »[15]. « *Des acteurs de tous types, ne disposant pas de base industrielle* »[16], peuvent « *se doter de moyens avancés* »[17]. Par exemple, les groupes pratiquants une insurrection armée (terroristes, groupes armés paramilitaires) qui n'ont pas les moyens, et n'ont pas besoin d'armes aussi sophistiqués tels que l'arme nucléaire ou des avions de chasse, peuvent aujourd'hui puiser dans des technologies offrant le même gain opérationnel que les grandes armées : drones, transmissions cryptées, cyber attaque,…

Un « pivot stratégique » a été effectué. Avec cette démocratisation technologique, source d'opportunités et de vulnérabilités nouvelles, l'hégémonie des grandes armées étatiques est remise en cause. Dans le domaine numérique, « *les États contribuent directement à ces évolutions en diffusant des armes cybernétiques qui, une fois connues, peuvent être étudiées, retravaillées et réutilisées* »[18]. Internet est aujourd'hui l'arme la plus accessible, au potentiel incalculable et qui bouleverse l'ordre établi. « *C'est comme si, dans le monde physique, une cible pouvait ramasser le missile tombé dans son jardin, et le réutiliser contre quelqu'un d'autre. Au premier rang de ces pays mauvais élèves , on devine les États-Unis …, dont l'agence de sécurité nationale, la NSA, s'était fait voler en 2016 des armes informatiques qui ont été utilisées en 2017 dans le cadre de vastes cyberattaques contre des centaines de millions d'internautes* »[19].

13 Revue stratégique de défense et de sécurité nationale 2017, page 33.
14 *Id.*
15 *Idid.*, page34.
16 *Id.*
17 *Id.*
18 *Idid.*, page 35.
19 GUERRIC PONCET, *Le salut des armées passera par l'ultra high-tech et le cyber*, Le point, 17/10/2017.

2. La résilience « hors limites »[20] des groupes armés modernes

La sophistication et la diffusion des technologies qui accompagnent la mondialisation offrent à des groupes pratiquants une insurrection armée une source grandissante de résilience. Ne disposant pas de base industrielle et scientifique, ces acteurs asymétriques bénéficient pour un investissement dérisoire (de quelques centaines à quelques milliers d'euros) de technologies avancées, naguère détenues par les seuls Etats (drones, cryptographie, navigation GPS, réseaux de communication et outils informatiques). La prolifération, dissémination et détournement (modes d'action artisanaux combinés à des méthodes innovantes comme des engins explosifs improvisés sur drones), de ces hautes technologies tend à niveler les rapports de force entre « forts » et « faibles », et à accroître de manière préoccupante la résilience d'acteurs asymétriques que certains qualifient « d'insurrection connectée ». Ces derniers ont aujourd'hui entre leurs mains un potentiel technologique capable de neutraliser l'avantage du « fort », jusqu'à leur conférer un caractère d'invincibilité dans certains contexte. « *C'est le combat du lion contre la mouche* »[21].

Malgré les frappes et les dommages causés par des grandes armées étatiques présentées technologiquement et opérationnellement supérieures, la capacité d'acteurs de 2nd ordre à se régénérer, se recomposer et à maintenir leur développement amène à étudier qui sont ces belligérants et sur quels piliers reposent leur résilience. Si leurs piliers peuvent être conceptualisés et identifiés, il devient alors aisé de comprendre dans quelle mesure les nouvelles technologies cimentent et fortifient ces piliers. Et cela permet finalement de mettre en lumière leur effet « *multiplicateur de résilience* »[22], et les perspectives qu'elles offrent par la diversité de leur nature et le tempo de l'évolution technologique qu'elles imposent.

2.1. Les « techno-belligérants » du 21ème siècle

Syrie, Irak, Nigéria, République Centrafricaine, Libye, Liban sud, Mali, Bangladesh, Turquie, Somalie, zone sahélo-saharienne, péninsule arabique et zone afghano-pakistanaise …

Sur fond d'états fragiles ou faillis, la multiplication des pays au sein desquels des groupes armés remettent en cause l'ordre établi et n'hésitent pas à lancer des attaques contre des armées régu-

20 Expression détournée issue de l'ouvrage *La guerre hors limites*, des colonels chinois Qiao Liang et Wang Xiandsui.
21 Bertrand BOYER, *op. cit.* , page 166.
22 Expression détournée, initialement utilisée mettre en avant l'effet multiplicateur de supériorité opérationnelle obtenu grâce aux nouvelles technologies.

lières s'inscrit dans la durée. Ces conflits embrasent de nombreuses sous-régions, opposant aux forces de grandes armées étatiques un ennemi fréquemment qualifié d'hybride. Il nous faut considérer et appréhender cette géographie des crises comme un système dont chaque groupe, cellule ou individu peut potentiellement interagir avec les autres, dont le centre de gravité est susceptible de se déplacer. Ceci impose d'abandonner une vision segmentée des crises et de discerner la stratégie globale de ces dernières dont il est évident qu'elle repose sur des outils technologiques capables de bouleverser le cadre espace/temps.

La démocratisation et prolifération des groupes armés et terroristes

Il n'y a pas de signes que ce type de menace, affiliée globalement à la menace terroriste, puisse décliner à court ou moyen terme. Spécialiste des mouvements djihadistes, Mohammad-Mahmoud Ould Mohamedou, directeur-adjoint du *Geneva Centre for Security Policy* et professeur associé au *Graduate Institute* en Suisse, n'hésite pas à évoquer qu'on l'assiste à « *la démocratisation du terrorisme* »[23]. On peut même observer que celle-ci se développe de façon inquiétante, et se diffuse sur le plan géographique jusqu'à frapper le territoire de grandes puissances étatiques, dont notamment les pays occidentaux qui peinent à les éliminer totalement aussi bien sur les théâtres d'opérations que sur leur propre sol national où des ramifications apparaissent. Au Sahel, le général français Bruno Guibert commandant la force « Barkhane » constate : « *l'ennemi est beaucoup plus dilué, il a adapté ses actions, et nous avons du mal à identifier des katibas [groupes armés], réduites à une dizaine de combattants* »[24].

Al-Mourabitoun, Ansar al-Charia, Ansar Dine, Al-Qaïda au Maghreb islamique, Boko Haram, Chebabs, Abou Sayyaf, Jemaah Islamiyah, Ansar Beït al-Maqdess, Front al-Nosra, …. La liste des groupes armées, ou des personnes isolées ou petits groupes se revendiquant de ces organisations, ne semblent pas avoir de fin grâce à leur « *capacité prolifération et de dilution* »[25]. Touchant tous les continents et ne connaissant aucune frontière, leur prolifération et développement ne trouvent pas de frein malgré celui que les grandes nations leur opposent.

23 Mohammad-Mahmoud Ould Mohamedou, interview du journaliste Frédéric Koller, Le Temps, 26 juillet 2016.
24 Nathalie Guibert, *Paris veut sortir « Barkhane » du piège malien*, Le Monde, le 15/11/2017.
25 Général Didier Castres.

L'élimination régulière de ces combattants irréguliers, de leurs principaux coordinateurs et décideurs, fait régulièrement la une de l'actualité mais cela ne change rien, comme les victoires éphémères de l'armée française au Mali. Ce caractère de résilience plonge le camp des démocraties et grandes nations dans un combat perpétuel, tel Sisyphe et son rocher…

Des acteurs asymétriques hybrides

Ne se limitant pas à la surface d'un État, les belligérants irréguliers, ou Groupes Armées Terroristes (GAT), recyclent les innovations technologiques du monde civil pour parvenir à leurs buts, souvent politiques ou religieux, tout en préservant leur structure. Ce type de belligérants, individus isolés ou petits groupes, dispose grâce aux nouvelles technologies et dernières innovations sur le marché d'une certaine capacité opérationnelle indépendante et surtout d'une capacité de résilience qui rend difficile leur éradication. Grâce au pouvoir « *égalisateur de l'électron* »[26], des acteurs non étatiques rivalisent désormais avec des États.

Atouts pour la surprise dans le temps, l'espace et les modes d'action, les nouvelles technologies leurs permettent de s'adapter à leur environnement et de s'y fondre tel le caméléon. A l'instar de la pieuvre, elles les autorisent également à développer un réseau tentaculaire agile et résistant, contournant et frappant où il veut. Et elles leur confèrent une faculté de résurgence et de renaissance tel le phénix sur n'importe quel point du globe. Ce « *techno-belligérant* »[10] hybride, apparemment matériellement insignifiant, inscrit durablement son action dans un type de conflit asymétrique que l'on peut qualifier de « *techno-guérilla* »[27.]

S'il est important d'identifier et cerner ces belligérants irréguliers, l'étude plus en détail des piliers de leur résilience, à l'ère du tout numérique et des technologies de rupture accessibles, permet de mieux réaliser à quel point ils peuvent adapter leur dispositif, et devenir suivant le contexte malheureusement invincible.

26 Référence à la déclaration du chef d'état-major de l'armée de Terre en 1992, le général d'armée Monchal qui déclarait qu'« *à l'avenir, le maître de l'électron l'emportera sur le maître du* feu ».
27 Issue du concept de techno-guérilla du lieutenant-colonel Guy Brossollet, auteur de *Essai sur la non-bataille*, 1976.

2.2. Conceptualisation de la résilience des groupes armés

L'idée de résilience n'est pas nouvelle et le rappel de la définition de cette qualité au premier sens est un prérequis indispensable. Dans la médecine traditionnelle chinoise, la résilience désigne la capacité des êtres vivants à se purifier et se rétablir face à la maladie. En physique, elle illustre la capacité d'un matériau à retrouver sa forme originelle après avoir subi une déformation. En psychologie, elle décrit la capacité d'une personne à faire face aux traumatismes et à rebondir face aux épreuves de la vie. Etendue aux organisations et entreprises, elle désigne la capacité à se rétablir et à assurer son développement en dépit des crises ou dommages subis.

Dans *Les canaux de la confiance. La résilience des petits groupes*, le colonel Vincent Gelez traite de la résilience des petits groupes armés. Il arrive à la conclusion que ces groupes sont résilients car ils bénéficient d'une « *structure endogène et exogène, souple* » qui leur permet « *tout à la fois d'exister, d'être permanent, et d'être capable d'absorber les chocs, de se déformer sans cesser d'être identique* »[28]. Cette approche nous permet de commencer à comprendre ce qu'est la résilience, et ce qu'elle évoque au premier abord lorsqu'on se penche sur les groupes armés sans regarder à ce niveau l'apport supplémentaire des nouvelles technologies.

Une résilience moderne

En ce début de 21ième siècle à la tête des forces armées américaines en Afghanistan et Irak, le général américain Petraeus a été confronté avec ses troupes à des acteurs irréguliers ayant bénéficié de la diffusion des technologies accompagnant la mondialisation. Dans la préface de la réédition de *Contre-insurrection théorie et pratique* de David Galula, il constate amèrement que « *les insurrections ont changé au cours des 45 dernières années; elles sont devenues encore plus dangereuses, dans un monde dont l'urbanisation et la globalisation ont accru le pouvoir et l'influence de groupuscules* ***autrefois voués à disparaître***. »[29]. Cet aveu nous amène à prendre la mesure qu'entre hier et aujourd'hui, ces groupes auraient bénéficié d'un élément supplémentaire qui leur permettraient de résister et de conjurer leur disparation en dépit des efforts des grandes armées étatiques qui étaient certaines de leur force et de leur disposition à les éradiquer.

28 Colonel Vincent Gelez, *Les canaux de la confiance. La résilience des petits groupes*, Revue inflexions, n° 29, 2015.
29 David Galula, *Contre-insurrection Théorie et pratique*, Economica, Préface du général David H. Petraeus et du lieutenant – colonel John A Nagl.

Une résilience structurée

A l'heure du tout numérique et des technologies high-tech accessibles, les *« techno-belligérants»* semblent bénéficier d'une résilience « *hors limites* »[30], et présenteraient une dimension « *indestructible* », une résilience organisée face aux coups et chocs portés par les grandes armées étatiques. A partir de ce constat, leur résilience pourrait être perçue comme un système plus complexe qu'en apparence, un système structuré sur lequel une étude systémique pourrait permettre de découvrir les sous-ensembles et de mesurer dans quelle mesure leur résilience serait supérieure aux grandes armées étatiques.

En commençant à décomposer la capacité des groupes armés à résister aux chocs, le principal caractère qui ressort, c'est la simultanéité et l'imbrication de différentes capacités. L'étude successive et séparée de chacune d'elles a nécessairement un caractère très artificiel mais elle permet d'appréhender ces capacités comme les véritables piliers de leur caractère « *d'invincibilité* ». Si ces piliers peuvent être conceptualisés et identifiés, il devient alors aisé de comprendre dans quelle mesure les nouvelles technologies cimentent et fortifient ces piliers et donc leur résilience.

2.3. Les piliers de la résilience des groupes armés

La résilience des groupes armés (terroristes, groupes armés paramilitaires) peut se référer à une capacité d'adaptation et de reconstruction continuelle portée et soutenue par une combinaison idéale de piliers. Cette combinaison de piliers s'inscrit dans une double approche défensive et proactive :

- une approche défensive en recherchant la discrétion dans la manœuvre et en anticipant les actions et réactions de son adversaire pour rester maître de ses mouvements. Cette approche vise un principe intemporel de la guerre, à savoir la liberté d'action[31] ;
- Une approche proactive en recherchant l'adaptation et l'agilité de son dispositif pour préserver ses ressources. Cette approche vise également un autre principe intemporel de la guerre, à savoir ici l'économie des forces.

Dans cette double approche, quatre piliers peuvent être identifiés et étudiés pour saisir l'apport des dernières technologies dans l'effet « *multiplicateur de résilience* »[32].

30 Expression détournée issue de l'ouvrage *La guerre hors limites*, des colonels chinois Qiao Liang et Wang Xiandsui.
31 Maréchal Ferdinand Foch, *Des principes de la guerre*.

2.4. Les piliers de résilience de l'approche défensive

Dans l'approche défensive, qui tient plus aux mesures de précaution et de gestion préventive du risque pour se tenir éloigné du choc potentiel et gagner en liberté d'action dans sa manœuvre, on trouve deux piliers : le **pilier informationnel** et le **pilier organisationnel**.

Pilier informationnel

Le pilier informationnel englobe la faculté à obtenir du renseignement opérationnel et du renseignement d'ambiance qui permet de se mettre à l'abri des surprises. Ce pilier permet de manœuvrer à tout moment en anticipant les actions et postures de son adversaire. Les groupes de combattants peuvent capter de l'information nécessaire à leur cycle décisionnel pour valider les moyens à utiliser et les buts à atteindre. Mais ils peuvent également déceler les menaces, l'inattendu, et apprécier les intentions de leurs ennemis. Plusieurs technologies vont leur apporter ce renseignement.

Dans une dynamique de veille passive, ils vont bénéficier de technologies pour rester informés sur le panel et le potentiel des outils high-tech à leur disposition et également sur les capacités et objectifs des grandes armées étatiques. En novembre 2015 grâce aux technologies de l'information, Daesh a mis en accès libre sur Internet le livret « *Safety and Security guidelines for Lone Wolf Mujahideen and small cell »*. Dans ce fascicule, les belligérants qui souhaitent commettre un attentat sont tout simplement invités à se tenir informés des rapports et analyses émis par les occidentaux eux-mêmes pour les comprendre et gagner en efficacité : « *…l'ennemi lui-même te montre comment l'attaquer, il te donne des idées et te guide. Dans les mots mêmes de l'ennemi, tu peux découvrir ses peurs, tu peux identifier ses points faibles, ses problèmes, et tirer avantage de tout ça dans tous les différentes étapes de la préparation de ton opération. Il y a quelques jours, je lisais un rapport écrit par des officiers de services de renseignement de plusieurs pays qui avaient analysé plus de 10 simulations d'attaques. Gloire à dieu, au fur et à mesure que je lisais, j'avais des idées encore plus imaginatives et créatives. Ils pensent même à des choses auxquelles nous ne pensons pas, et dès que nous parvenons à découvrir ce à quoi ils s'attendent, nous pouvons l'utiliser à notre profit et contourner leurs plans…* »[33].

32 Voir annexe.

33 Abu Ubdullah al-Adm, *Safety and Security guidelines for Lone Wolf Mujahideen and small cells* , page 11.

Dans une dynamique de veille active, ils vont chercher à anticiper les actions de leurs ennemis en décelant sur le terrain leurs intentions grâce également à des outils détournés tel que le drone civil. Ce capital informationnel leur offre un « capital survie » indéniable, et en fait un adversaire fugace, renseigné et abrité ayant souvent l'initiative dans l'action.

Pilier organisationnel

Ensuite, le pilier organisationnel offre la faculté de rendre le groupe de combattants moins vulnérable aux ruptures en développant leurs forces morales. Ce pilier est le fondement d'une organisation tentaculaire résurgente (capacité de s'entretenir et se régénérer rapidement en frappant à n'importe quel endroit, tel la pieuvre avec ses tentacules). Il permet de développer son dispositif efficacement en bénéficiant de la fulgurance sans tenir compte de l'environnement, des circonstances et de son adversaire.

Des technologies vont leur permettre de diffuser leur idéologie grâce à une propagande devenue une véritable arme de guerre. Cette capacité fédère, soude et amène de nouvelles ressources organisationnelles. Elle évite l'émiettement et la désagrégation de leur organisation dans le combat mené. L'emploi de la propagande a toujours fait partie des moyens déployés par les belligérants lors d'une guerre. Maintenir le moral des combattants, recruter des alliés et soutenir les initiatives personnelles et collectives sont des fonctions classiques. Mais à l'aube du 21ième siècle, les nouvelles technologies ont simplifié et amplifié d'une manière inégalée cette capacité à capter et souder les ressources de l'organisation. Elles maximisent la solidité du pilier organisationnel et *in fine* la résilience des groupes armés.

2.5. Les piliers de résilience de l'approche proactive

L'approche proactive tient plus aux mesures de recherche et d'appropriation de solutions nouvelles et de renouvellement des modes d'actions visant à économiser les forces. En gardant un temps d'avance sur la menace, on permet à son dispositif de durer dans la manœuvre, et dans un combat basé sur le temps long. Dans cette approche, on trouve deux piliers : le **pilier opérationnel** et le **pilier structurel.**

Pilier opérationnel

Le pilier opérationnel englobe la faculté de s'adapter tactiquement pour être mieux protéger à l'avenir sur le « terrain ». L'appropriation de nouveaux outils et des retours d'expérience des actions récentes permet de d'optimiser son dispositif et de trouver le meilleur rapport capacités/effet pour atteindre son objectif en préservant ses ressources.

Pour être plus résilients, les belligérants ont appris à tirer les leçons des chocs auxquels ils ont dû faire face. Ils ont appris par eux-mêmes. Inscrit dans une approche pragmatique, ce pilier offre une capacité de renouvellement, d'appropriation de nouveaux outils et modes d'actions. Ce renouvellement opérationnel cherche à développer de nouveaux modes d'actions, à repenser les outils existants et expérimenter de nouvelles façons de faire. L'utilisation de smartphones avec des applications cryptées a permis aux groupes armés de s'affranchir des simples téléphones mobiles facilement écoutables et traçables qui bien souvent concouraient à leur destruction. L'emploi de drones civils détournés et piégés les met également à distance d'une capacité de riposte qui peine à localiser leurs ressources et à les neutraliser efficacement et définitivement. Ce processus de « régénération opérationnelle » vise à saisir les opportunités de résilience. Elle s'accompagne d'une attention focalisée sur l'utilisation optimales des ressources disponibles et à la limitation de la prise de risque, compte tenu du potentiel de destruction de leurs adversaires.

Pilier structurel

Le pilier structurel fait ici référence à l'agilité et à la souplesse de la structure même des groupes armés. Il désigne leur « *structure coalescente* »[34] (capacité de se structurer rapidement et à n'importe quel endroit à partir de ressources non-structurées, telles des gouttes de mercure éparpillées qui s'assemblent rapidement en un point donné). Cette structure permet de préserver son dispositif grâce à une agilité dans la manœuvre d'attaque qui devient difficilement détectable jusqu'au dernier moment avant le regroupement et l'attaque malgré les capacités de détection et de riposte de son adversaire.

Malgré une apparence déstructurée (image de l'individu isolé ou du groupe disséminé), les dernières technologies dont notamment le numérique (messageries cryptées) autorisent cette coalescence à leur structure, cette réactivité et capacité de contournement de la menace.

34 Stéphane Dossé, Olivier Kempf, *Stratégies dans le cyberespace*, cahier de l'AGS N°2, L'esprit du livre, 2011.

Cela engendre une menace diffuse presqu'impossible à parer et à neutraliser. Cela se rapproche de la méthode allemande *« auftragstaktik »* théorisée au début du XIXème siècle. En laissant l'autonomie aux exécutants sur le terrain, en diffusant un plan compris de tous les exécutants et valorisant l'initiative, ce principe confère souplesse, discrétion, agilité et renforce leur résilience.

Maintenant identifiés et étudiés, ces quatre piliers permettent de comprendre l'effet « *multiplicateur de résilience* ». Ils conduisent finalement à une analyse attentive des différentes technologies et des perspectives qu'elles offrent dans le développement de la résilience des groupes armés.

2.6. Le drone, « le meilleur ami du terroriste »[35]

Le drone, « *le meilleur ami du terroriste* ». Cette expression n'a jamais été aussi vraie que sous le prisme de la résilience offerte à ces utilisateurs. En effet avec son *modus operandi* sans limites techniques, législatives et doctrinales aux mains de petits groupes armés, le drone permet efficacement d'être plus résilients que de grandes armées étatiques. On peut même parler d'invincibilité ponctuelle quand le drone met à l'abri à bonne distance de riposte les opérateurs. Il préserve et renforce les groupes armés en renforçant 3 piliers de leur résilience, et en suivant les grands principes stratégiques d'économie des forces et de liberté d'action.

Le drone

Avant d'étudier les différents apports du drone dans la résilience d'acteurs asymétriques, il convient de définir ici même l'objet de ce chapitre. Arme des temps modernes, les drones sont associés, outre-Atlantique, à la « sale guerre », aux frappes militaires dites chirurgicales de grandes armées étatiques telle que celle des Etats-Unis. Leurs noms souvent cités dans l'actualité ne laissent aucun doute sur l'emploi de telles machines : « *reaper* » (la *faucheuse*) ou encore « *predator* » (*prédateur*). Cependant, ces armes des temps modernes ne sont pas celles que les groupes armés vont avoir à leur portée et utiliser. Comme Internet ou le GPS, les drones sont des équipements initialement apparus pour répondre à des objectifs militaires avant de tomber dans le champ des applications civiles, et dans les mains de « Monsieur tout le monde ».

35 Sous la direction d'Olivier Entraygues*, L'âge du drone*, Polémoscopie n°2, Le Polémarque, page 63

« *Un drone aérien se définit comme un engin volant sans aucune personne à bord, télépiloté ou programmé, pouvant emporter une charge utile. Il est en principe récupérable en fin de vol et peut être réutilisé* »[36]. Cette technologie a été démocratisée par la mondialisation et comme le constate le lieutenant-colonel Olivier Entraygues, « *ce qui n'était au début qu'un objet de loisirs a pénétré avec une versatilité déconcertante le champ de bataille moderne* »[37]. De plus, une approche résolument ludique de son utilisation a permis sa prolifération :

- nouvelle façon de prendre des photos en embarquant caméra et appareil photo ;
- nouveau loisir basé sur des compétitions et courses de drones grand public ;
- interconnexion avec tablette et téléphone portable grand public pour apprendre à piloter « à la maison » et bénéficier de toutes leurs capacités.

Un économiseur de forces et de ressources

Utilisé dans une attaque cinétique, le rapport « ressources organisationnelles consommées / effet sur l'objectif » est idéal pour les groupes armés cherchant à s'en prendre à des grandes armées étatiques. Délaissant les attaques suicides ou à caractère suicidaire (au regard du rapport de force entre belligérants et armées étatiques), le drone civil grand public détourné de son usage récréatif permet en tant qu'arme à distance de préserver les combattants insurgés, et de s'abriter à bonne distance de l'attaque.

Evoquant cette nouvelle arme aux mains de terroristes, Alexandre Vautravers, rédacteur en chef de la *Revue militaire suisse*, souligne que « *des drones vendus en magasin entre quelques centaines et quelques milliers de francs sont conçus pour transporter des appareils photo de 800 grammes à 4 kilos. Il est facile d'y fixer une grenade à main, qui ne pèse que 500 grammes, et de leur adjoindre un mécanisme de déclenchement par téléphone portable* »[38].

Cette utilisation de drone n'est pas de la science-fiction. Comme l'avait malheureusement prédit le lieutenant-colonel Olivier Entraygues, le drone est devenu un « *engin explosif improvisé volant* »[39], et une des technologies préférées des groupes combattants.

36 Sous la direction d'Olivier Entraygues, *op. cit.* , page 63.
37 *Id.*
38 Etienne Dubuis, *Les drones miniatures, une nouvelle arme aux mains des terroristes*, Le Temps, 9/03/2015.
39 Sous la direction d'Olivier Entraygues, *op. cit.* , page 68.

De nombreux drones et ateliers de préparation ont ainsi été découverts en Irak et Syrie lors de l'avancée de la coalition internationale pour repousser et neutraliser les combattants de Daesh entre 2016 et 2017[40]. L'organisation non-gouvernementale *Conflict Armament Research (CAR)* affirme avoir découvert à Ramadi, une ville libérée en février 2016 par l'armée irakienne, un atelier de drones de Daech[41]. De plus, comme le révélait Le Monde, l'attaque réalisée le 2 octobre 2016 à Erbil en Irak avec un drone piégé qui a grièvement blessé deux commandos français, et coûté la vie à deux peshmergas, « *a apparemment été commise avec un banal appareil grand public* »[42]. Il transportait une charge explosive qui a été déclenchée lorsque les militaires l'ont intercepté.

Extrapolé à un autre milieu, le 30 janvier 2017, la première utilisation d'un drone naval piégé a été mentionné dans *Defense News* par Kevin Donegan, commandant de la Cinquième flotte américaine basée à Bahreïn[43]. Les rebelles du Yémen auraient donc réussi à importer et adapter l'utilisation du drone au milieu maritime en télé opérant un navire bourré d'explosifs. La frégate saoudienne de classe Al Madinah naviguait en Mer rouge lorsqu'elle a été attaquée par les rebelles houthis.

Anticiper la menace pour se préserver

« *Des drones non armés équipés d'une caméra peuvent également servir à des actions terroristes* »[44]. Fort de sa capacité informationnelle, le drone grand public équipé d'une caméra ou d'un appareil photo est un multiplicateur de résilience bon marché. C'est un allié idéal dans un dispositif de protection et d'anticipation de la menace : « *Le drone civil est un moyen low-cost - high-tech permettant d'obtenir ponctuellement un renseignement de qualité sans être décelé. Aucune modification du système n'est nécessaire pour qu'il soit utilisé dans ce cadre* »[45].

Sans aucune modification, il permet en effet de recueillir des informations précises sur des installations sensibles ou des troupes au sol qu'il s'agisse de connaître leurs déplacements, dispositif, ou d'identifier leurs matériels. Des photos aériennes permettent par exemple de déterminer l'emplacement précis de pièces d'artillerie ou positions des forces adverses. Des films aériens peuvent transmettre en temps réel le mouvement de véhicules, de troupes en approche.

40 http://robots.blog.lemonde.fr/2016/11/15/un-peu-plus-dinfos-sur-les-drones-de-letat-islamique/, consulté le 11/11/2017.
41 Christophe Lamfalussy, *Un atelier de drones de Daech découvert en Irak*, La libre Belgique, 19/10/2016.
42 Jean-Michel Normand,Le Monde, *Le drone de loisir, nouvelle arme du terrorisme ?*, 11/10/2016.
43 Guerric Poncet, *Une frégate saoudienne frappée par un drone naval houthi*, Le point, 23/02/2017.
44 Etienne Dubuis, *op. cit.*
45 Sous la direction d'Olivier Entraygues, *op. cit.* , page 68.

Ainsi, le 23 août 2014, les combattants islamistes de Daesh « *ont posté sur YouTube une vidéo de 14 minutes (aujourd'hui supprimée) montrant comment avec un simple drone grand public made in China (DJI Phantom FC40[46])* »[47] ils avaient réalisé « *un repérage aérien de la base aérienne* »[48] située au nord de la ville de Raqqa en Syrie pour estimer sa défense avant de l'attaquer et de s'en emparer. Le tout pour 450 euros...

L'outil idéal pour la propagande et le développement de la résilience

« *Depuis quelques mois, les services de propagande de l'EI diffusent des images, filmées par des caméras embarquées, d'obus ou de grenades lâchées avec précision par des drones sur des blindés de l'armée irakienne, des rassemblements de soldats ou des convois de 4x4. On peut voir la munition, équipée d'ailettes ou même de plumes de volants de badminton, tomber en oscillant sur plusieurs centaines de mètres, puis exploser en touchant le sol ou un véhicule. Même s'il est évident qu'ils ne sélectionnent pour la mise en ligne sur internet que les coups au but, qui doivent être rares, l'effet est dévastateur* »[49].

Le drone devient ici une arme de guerre redoutable. Il offre un support visuel considérable à la propagande des groupes armés. Certes ces images font peur à tout monde mais pour les groupes armés, elles permettent de favoriser le développement de leur organisation. Grâce une propagande friande de ce genre d'image, ces supports visuels issus de drones contribuent à forger la force morale des combattants, à recruter de nouvelles ressources, à soutenir les initiatives personnelles et collectives, et *in fine* contribuent à leur résilience. Tout en terrorisant ces détracteurs et séduisant ses sympathisants, les groupes de combattants grossissent leurs rangs, trouvent de nouveaux relais et développent leur capacité de résurgence en n'importe quel point du globe.

Une furtivité inégalée au service de la résilience

« *Caractéristique héritée de leur origine militaire, les drones sont également très furtifs* »[50].

46 Piloté à distance, ce type de drone utilise des coordonnées GPS prédéterminées, et est généralement utilisé pour filmer des mariages ou des paysages. N'importe qui peut en commander un sur Internet.
47 Judikael Hirel, *Syrie : l'EI conquiert une base grâce à un drone à 450 euros*, Le Point, 31/08/2014.
48 Judikael Hirel, *op. cit.*
49 AFP, *Les drones de l'EI inquiètent l'Occident*, La tribune de Genève, 3/03/2017.
50 Monsieur le sénateur Bruno SIDO et monsieur le député Jean-Yves LE DÉAUT, fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, *Les drones et la sécurité des installations nucléaires*, Rapport n° 267 (2014-2015) du Sénat, , déposé le 29 janvier 2015, Introduction.

Leur empreinte visuelle, acoustique et radar octroient une grande furtivité. Cette capacité offre un atout supplémentaire dans la résilience des groupes armés. En France durant la vague des survols des centrales nucléaires et des bases aériennes entre 2014 et 2015, des drones ont semé la panique. Leur furtivité ont permis de ne pas pouvoir les tracer et remonter aux pilotes. Il n'y a pas eu possibilité d'imputer réellement ces actions à un groupe donné ou à des terroristes potentiels.

Leur furtivité est considérable. Ils peuvent être utilisés hors de la vue du pilote grâce au radio pilotage et à l'utilisation du retour caméra. Pouvant utiliser la technologie de guidage par GPS (non traçable), ces machines peuvent fonctionner de manière autonome en suivant des itinéraires préprogrammés. De plus, ces appareils sont difficiles à détecter par les radars, et ils offrent une taille indétectable à l'œil nu lorsqu'ils sont dans les airs (de 40 centimètres à un mètre d'envergure). Le lieutenant-colonel d'Olivier Entraygues souligne d'une part que les capteurs optiques de génération « 4K » permettent aux drones de prendre des vues à distance aisément même à plus de 100 mètres et qu'« *il est impossible de détecter un drone si on ne sait pas où regarder* »[51]. D'autre part, il conforte que la furtivité est renforcée par la motorisation des drones : « *la multiplication de mini-moteurs électriques réduit la signature acoustique par rapport à un moteur unique* »[52].

La difficulté à les détecter et à remonter aux combattants est renforcée d'autant plus qu'« *en Irak les opérateurs de drones sont souvent des djihadistes venus de pays occidentaux, habitués aux commandes de jeux vidéos* »[53], et extrêmement talentueux dans le pilotage en discrétion. Dans un rapport publié le 31 janvier, le *Combating Terrorism Center* de l'école militaire américaine de West Point, écrit, sur la base de documents de l'EI saisis en Irak, que «*l'EI a mis en place une unité de drones formelle, institutionnalisée, financée depuis 2015, sinon plus tôt* »[54].

2.7. « Le cyber, empire de l'asymétrie »[55]

La démocratisation et la globalisation des technologies de l'information ont joué un rôle central dans le nouvel ordre numérique actuel. En effet, la transformation digitale de la société a contribué à faire émerger un nouvel empire : « l'empire cyber ».

51 Sous la direction d'Olivier Entraygues, *op. cit.*, page 68.
52 *Id.*
53 AFP, *op. cit.*
54 http://www.lefigaro.fr/flash-actu/2017/01/31/97001-20170131FILWWW00261-les-drones-tueurs-de-l-ei-de-plus-en-plus-efficaces.php, consulté le 31/01/2018
55 GUERRIC PONCET, *Le salut des armées passera par l'ultra high-tech et le cyber*, Le point, 17/10/2017.

Cet « *empire de l'asymétrie* » est le milieu d'évolution le plus propice aux groupes armés pour nuire tout en simplifiant et décuplant leur capacité de résilience. Dans ce monde virtuel où les possibilités de « se camoufler » et de « s'embusquer » sont considérables, les acteurs asymétriques, jusqu'alors isolés du reste du monde, utilisent à dessein le cyber pour recruter, endoctriner, se renseigner, communiquer, s'organiser, planifier voire frapper (avec des cyberattaques) en minimisant le risque d'être neutraliser dans le monde réel.

Sur le plan stratégique, cet empire cyber contribue à renforcer directement les 4 piliers[56] de la résilience (conceptualisés dans ce mémoire) des groupes armés d'une manière inégalée. Il offre le plus large spectre d'actions juxtaposables et combinables qui leur permet de se régénérer, se recomposer et se développer en dépit des efforts des grandes armées étatiques qui tentent de les éradiquer réellement et virtuellement. Tels de métastases invasives, les groupes armés se développent et semblent indifférents aux coups portés. Ce niveau de résilience était jusqu'à alors impensable : « *The Internet revolution has allowed terrorist groups to obscure their operations in new ways that complicate the old way of thinking about threats* »[57].

Le renseignement d'origine cyber : ciment du pilier informationnel

Portes ouvertes sur le monde, les outils numériques, via notamment Internet et ses réseaux sociaux, offrent une source d'information et de renseignement sans limites qui contribuent au dispositif de protection des groupes armés. En effet, la résilience des groupes armés réside en partie dans leur aptitude à anticiper et détecter les menaces qui pourraient les frapper. Et cette aptitude est exacerbée dans le cyber.

La plupart des groupes armés sont rôdés à l'utilisation massive des réseaux sociaux (Facebook, Twitter, Instagram, YouTube, Whatsapp, Viber, Flikr...) pour des besoins évidents de communication et de propagande mais également pour des besoins de renseignement. Activité beaucoup plus discrète mais tout aussi intense. Ces « *hirondelles numériques* »[58], comme les surnomme le lieutenant-colonel Bertrand BOYER, se sont fait maîtres dans la collecte de données recueillies sur les profils des soldats des grandes armées étatiques eux aussi rôdés à l'utilisation des réseaux sociaux.

56 Voir annexe.
57 P.W. Singer et Allan Friedman, *Cybersecurity and cyberwar*, Oxford University Press, page 101.
58 Bertrand BOYER, *op. cit.* , page 154.

Mais bien souvent, ces soldats sont inconscients du niveau de confidentialité des informations semées sur les pages de leurs profils, d'amis ou de leur famille. Des informations stratégiques contribuant à leur résilience peuvent être contenues dans de simples statuts, photos ou vidéos : heure de départ d'une patrouille, zone géographique d'intérêt, relève d'unités, installations bases secrètes[59] (à cause d'une application fitness en ligne)… Ces « *hirondelles numériques* » collectent passivement les informations sur les profils laissés ouvert à tout public, ou avec le concours de faux profils (jeunes filles avenantes ou sympathisants) pour leurrer leurs cibles. Les armées françaises ont même été conduites à éditer en 2012 une plaquette G*uide du bon usage des réseaux sociaux* pour faire face à ce phénomène qui semble difficilement régulable avec l'explosion du phénomène des blogs (lieux de publication d'individus), des forums de discussion (autour d'une thématique)…

Ces réseaux sociaux sont de vrais mémentos, voire guides documentés, pour les groupes armés. Ils constituent une source de renseignement à ne surtout pas négliger surtout au regard de l'intelligence de certains belligérants qui n'hésitent pas à croiser leurs sources de renseignement d'origine cyber. « *Pendant les opérations en Libye en 2011, les informations provenant d'un site de suivi du trafic aérien étaient corrélées avec les annonces de frappes sur le réseau Twitter en temps réel. Les différents belligérants pouvaient ainsi se renseigner sur les opérations aériennes menées par les forces de l'OTAN*» [60], et prendre leur disposition pour sécuriser leurs ressources organisationnelles.

Par le tempo de son évolution technologique, le cyber offre des perspectives de renseignement qui ne semblent pas avoir de limites :

- géolocalisation directement intégré sur les profils des soldats via leurs réseaux sociaux, et donc possibilité de localiser au mètre près la menace ;
- pratique du «data mining» (exploration de données) qui permet d'analyser le comportement des internautes au travers de leurs pratiques (recherches, consultations, profils créés, membres de forum). « *L'exploitation de « signaux faibles » à partir des informations générées par les réseaux sociaux et des traces mnésiques qu'elles laissent est une source de renseignement potentielle* »[61].

59 http://www.lefigaro.fr/secteur/high-tech/2018/01/29/32001-20180129ARTFIG00212-une-application-de-fitness-devoile-la-position-de-bases-militaires-secretes.php, consulté le 31/01/2018.
60 Réflexion doctrinale interarmées, *Réseaux sociaux, Nature et conséquences pour les forces armées*, RDIA-2013/001 RS(2013), N° 067/DEF/CICDE/NP du 19 avril 2013, page 19.
61 *Ibid.*, page 17.

« L'empire de la propagande » au service du pilier organisationnel

Pour accentuer leur résilience, les groupes armés, et en général toutes les insurrections, tirent un double avantage de la dimension mondiale du cyber. En effet, la vocation universelle d'Internet permet aux messages d'insurgés d'atteindre le plus grand nombre de personnes à l'échelle de la planète. D'une part en communication intra-organisationnelle, à destination de partisans ou de sympathisants, le vecteur cyber diffuse largement la propagande pour fanatiser les masses et développer la force morale de membres même isolés. D'autre part en communication externe, les groupes armés réussissent avec le cyber à manipuler les consciences, à endoctriner, à recruter et à densifier leur organisation sur et depuis n'importe quel point du globe.

Depuis « l'autre camp », le général américain David H. Petraeus identifie ce pouvoir en le mettant en perspective avec les théories du lieutenant-colonel Galula. « *Toutefois, la première nécessité dans les opérations de contre-insurrection moderne est d'une autre nature : il s'agit de conserver la maîtrise de l'information et des attentes de l'opinion ; Galula avait aussi vu cela, bien avant l'avènement de l'Internet. Les vidéos créées et aussitôt mises en ligne sur le cyberespace servent de campagnes de recrutement, de levées de fonds et d'opérations de propagande* »[62] et sont redoutablement efficaces.

Au travers de réseaux sociaux grands publics, des groupes armés, tel que la branche armée du Hamas, peuvent fanatiser leurs membres, voire d'autres groupes séduits par leur capacité de fédérer et souder les troupes. Ainsi, « *la branche armée du Hamas dispose-t-elle d'un compte Twitter suivi par près de 40 000 personnes (followers) : @alqassambrigade* »[63]. Au-delà de convaincre les adeptes de la puissance de leur organisation, la propagande cyber des groupes armés donne également tous les éléments psychologiques et opérationnels pour que n'importe quel membre soit le mieux « armé » possible. En démultipliant la force de caractère de combattants, leur résilience ne fait que croître sur le terrain.

C'est essentiellement grâce à une utilisation des moyens de communication modernes au service d'une propagande opérationnelle, que les groupes armés réussissent aussi à recruter et à convaincre de nouveaux adeptes de rejoindre leur organisation.

62 David Galula, *op. cit.* , Préface du général David H. Petraeus et du lieutenant –colonel John A Nagl.
63 Bertrand BOYER, *op. cit.* , page 154.

C'est une véritable arme de guerre. La propagande cyber valorise les parcours personnels, exploite les troubles mentaux, les carences affectives et spirituelles pour les mettre au service de la cause et des objectifs stratégiques. Cette dynamique de recrutement d'origine cyber renforce la cohésion d'un mouvement internationaliste ayant besoin d'un afflux permanent de ressources pour consolider ou remplacer les pertes. Sa résistance aux tentatives d'éradication se fortifie.

Le mode de diffusion « viral » et l'instantanéité des communications offertes par le cyber démultiplient la portée et l'impact de la propagande. Ces deux points clés concourent à capturer et maintenir des auditeurs dans l'instantanéité et l'émotion primaire. Ils jouent sur la fibre émotionnelle et créent une dépendance. De même, la capacité de véhiculer des messages, photos, vidéos sans aucune censure (glorification des massacres, du passage à l'acte,...) provoque chez ses adeptes un degré élevé de fanatisme, de violence et une propension à servir « jusqu'au bout ».

Le cyber source de liberté d'action et de résilience

Aujourd'hui, la supériorité opérationnelle et technologique des pays occidentaux est telle que personne ne peut les défier sur un champ de bataille classique. Pour un agresseur, les dommages seraient inacceptables voire irréversibles. Cependant un nouveau champ de bataille se dessine pour contourner cette fatalité. Le cyberespace permet à tous les types d'agresseurs, dont les acteurs asymétriques, de rentrer en confrontation avec des grandes armées étatiques sans subir de contre-attaques destructrices et donc garder une certaine capacité de résilience.

Comme l'officialise M. Jean-Yves Le Drian, ministre de la Défense en 2013, *« depuis 2008, le cyberespace est devenu un champ de confrontations à part entière* »[64]. La dissémination et la sophistication croissante des moyens d'agression numériques contribuent à l'intensification des attaques informatiques. En 2016, M. Jean-Yves Le Drian illustre lui-même ses propos de 2013 en annonçant que « *les tentatives d'agression informatique sur mon ministère doublent chaque année. En 2016, 24 000 attaques externes ont été bloquées par nos dispositifs de sécurité. Parmi celles-ci, quelques centaines, plutôt élaborées, avaient de véritables intentions de nuire* »[65].

64 M. Jean-Yves Le Drian, Ministre de la défense, *discours d'ouverture du colloque sur la cyberdéfense*, Rennes, 3 juin 2013.
65 http://www.lefigaro.fr/international/2017/01/08/01003-20170108ARTFIG00050-le-ministere-de-la-defense-a-dejoue-24000-cyberattaques-en-2016.php, consulté le 02/12/2017.

Malgré eux, « *les Etats contribuent directement à ces évolutions en diffusant des armes cybernétiques qui, une fois connues, peuvent être étudiées, retravaillées et réutilisées.* »[66]. Les groupes armés s'adaptent tel le caméléon en s'appropriant ces outils inespérés. Le cyber façonne un adversaire fugace et renseigné ayant souvent l'initiative dans l'action tout en s'abritant.

L'actualité de ces dernières années reflète bien l'approche proactive des groupes armés dans l'exploitation des armes cybernétiques « *faciles à mettre en œuvre, permettant des agressions discrètes, …, peu coûteuses et fortement perturbatrices* »[67] pour optimiser simultanément leur capacité de nuisance et de résilience. Les exemples ci-dessous illustrent bien que le cyber offre un des meilleurs rapports capacités/effet pour un groupe armé pour atteindre ses objectif en préservant ses ressources organisationnelles.

En France, suite aux attentats de janvier 2015, « *l'état-major français des armées a activé pour la première fois une cellule de crise cyber. … Le site Zataz.com a recensé plus de 19 000 actes hostiles sur des sites français les plus divers, et notamment le ministère de la défense* »[68]. Ces actes tous azimuts provenaient de nombreux groupes identifiés, notamment des groupes armés tel que *Cybercaliphate*, un groupe se revendiquant de l'Etat islamique. Quelques mois après en avril 2015, *Cybercaliphate* visait TV5 Monde en réussissant à stopper la diffusion de la chaîne, tandis que « *le piratage des comptes Twitter et Facebook entraînait la publication de messages hostiles à la France et à ses soldats* »[69], et la publication de CV de militaires français[70].

A l'étranger, les grandes armées pourtant réputées et craintes ont également subi des attaques cyber revendiquées par des groupes armés. En 2012, durant l'opération pilier de plomb des groupes palestiniens, comme les Brigades Ezzedine al-Kassam (la branche armée du Hamas) « *a prouvé qu'en dépit de l'asymétrie des forces en présence, il a pu répondre au coup par coup au cyber-attaques israéliennes* »[71].

66 Revue stratégique de défense et de sécurité nationale 2017, publié le 13 octobre 2017.
67 Directions des affaires stratégiques, *horizons stratégiques*, 2012, page 65.
68 Nathalie Guibert, *Cyberattaques : l'armée a activé pour la première fois une cellule de crise*, Le Monde, 17/01/2015.
69 Sous la direction de Flore de Feydeau , *Espace numérique, Un nouveau champ de bataille*, Armées d'aujourd'hui n° 415 Avril 2017, page 22.
70 Opex360.Com - 09 avril 2015 - Via une cyberattaque d'ampleur inédite contre TV5 Monde, l'État islamique menace les familles des militaires français, consulté le 04/12/2017.
71 http://www.geopolitique.net/fr/lutilisation-dinternet-et-des-reseaux-sociaux-lors-de-loperation-militaire-israelienne-a-gaza-en-novembre-2012/, consulté le 04/12/2017

Ils n'étaient pas en reste en tentant de contrer l'influence de Tsahal sur les réseaux sociaux[72]. En 2015, un groupe se réclamant de Daech a piraté les comptes Twitter et YouTube du Centcom[73], le commandement militaire américain au Moyen-Orient, dévoilant les coordonnées personnelles de militaires, et publiant : « *Soldats américains, nous arrivons. Surveillez vos arrières. Etat Islamique* »[74] et également « *Au nom de Dieu, le très bienveillant, le très miséricordieux, le Cyber Califat continue son cyberdjihad* »[75].

Vecteur d'une structure coalescente favorisant l'économie des forces

L'ingéniosité des groupes armés dans l'utilisation des nouveaux outils technologiques contribue à alimenter l'éternelle « histoire du glaive et du bouclier ». Aujourd'hui, cette histoire comporte des boucliers numériques qui ne cessent de s'accroître de par leurs nombres et formes : codes informatiques difficilement traçables, supports numériques protégés et facilement disséminables (disques durs, clé USB), smartphones avec applications de communication cryptée, infrastructures publiques de télécommunication facilitant la furtivité,…

Le cyber est partout, à portée de main de n'importe quel groupe ou organisation souhaitant valoriser l'initiative, l'agilité, l'autonomie et la préservation de ses ressources organisationnelles. Dans *La guerre hors limites*, les colonels chinois Qiao Liang et Wang Xiandsui avaient anticipé cette prolifération technologique et ses conséquences : « *aujourd'hui parce que les moyens sont nombreux et varient à l'infini, ce qui donne véritablement l'impression de voir un ennemi derrière chaque arbre. N'importe quelle direction, n'importe quel moyen, n'importe quel individu peuvent représenter une menace potentielle pour la sécurité nationale. Or, si cette menace peut être clairement ressentie, il est néanmoins très difficile d'établir immédiatement d'où elle vient* »[76].

Le cyber confère à une nuée d'acteurs une capacité à manœuvrer sur un espace immense et à y effectuer des transferts d'efforts sur des distances tout aussi importantes en toute discrétion.

72 http://www.opex360.com/2012/11/19/pilier-de-defense-israel-est-la-cible-de-millions-de-cyberattaques/, consulté le 04/12/2017.
73 AFP, *Le compte Twitter de l'armée américaine piraté par l'État islamique*, Le Point, 12/01/2015.
74 https://www.francetvinfo.fr/monde/un-groupe-se-reclamant-de-daech-publie-des-donnees-confidentielles-de-l-armee-us_1681179.html, consulté le 04/12/2017.
75 *Id.*
76 Qiao Liang, Wang Xiandsui, *op cit.*, page 167-168.

Cette structure résiliente peut être qualifiée de « *coalescente* »[77], telles des particules éparpillées insaisissables, qui savent se regrouper et fusionner au moment et au lieu opportuns pour agir avec surprise. Avec le cyber, les groupes armés peuvent donc choisir qui, où et quand frapper en :

1. facilitant leurs communications vers des cellules disséminées sur les zones cibles ;
2. restant dissimulés dans la préparation ou l'exécution de leurs actions ;
3. diminuant le risque de perturbations de leurs moyens de conduite et planification.

En effet, le cyber est un facilitateur de communication intra insurrectionnelle. Cela a un impact tactique immédiat. Le cyber permet de coordonner des actions, d'assurer le lien entre plusieurs groupes/individus, de faciliter les ravitaillements et de diffuser des ordres, ou explications sur les modes opératoires. Sous le prisme du cyber et de la connectivité numérique instantanée (Youtube, Facebook, Twitter, WhatsApp, Snapchat, Skype, iMessage, Viber, Telegram, etc.) les membres d'un groupe armé peuvent être vus comme des effecteurs, comme des organes récepteurs indépendants qui entrent en activité après avoir reçu un stimulus, une impulsion nerveuse. Cela donne une organisation en réseau structurée, redondante, très agile et efficacement redoutable.

Sur le temps court, ce « réseau nerveux » permet de combiner, recombiner et coordonner ses effecteurs vers leur ligne d'opération en évitant les coups avec agilité. Chaque effecteur conserve une relative autonomie en restant lié à son groupe armé, grâce au cyberespace qui met à disposition des outils (messagerie instantanée, réseaux sociaux, forums, téléphonie satellitaire, plateformes diverses,…) qui « *sanctuarisent l'individu dans une communauté … qui rend possible la coordination des opérations, seule gage d'efficacité dans un combat asymétrique* »[78]. De plus, dans ce type de structure sans hiérarchie apparente, la neutralisation ou capture d'un effecteur ne participe pas généralement à l'éradication du groupe ou à la mise au grand jour de sa structure.

Sur le temps long, des outils cyber comme les outils de stockage (clé USB, disque dur, ordinateur portable, ….) permettent de diffuser et disséminer des données stratégiques et tactiques de « main à la main », sans contrôle possible via les réseaux de communications. Des cartes, des plans, des guides de fabrication d'explosifs, des « vadémécums du combattant terroriste », des instructions qui permettent de conduire, planifier et soutenir des actions passent « sous le radar » des grandes armées étatiques.

77 Stéphane Dossé, Olivier Kempf, *op. cit*.
78 Bertrand BOYER, *op. cit.*, page 162.

En 2009, des soldats américains ont capturé un membre d'un groupe armé en Irak, et ont fait une découverte étonnante sur son ordinateur portable. Il avait à l'aide d'un logiciel gratuit sur Internet détourné le flux satellite de contrôle des drones et savaient ce que les américains surveillaient : « *the captured leader's laptop were « days ans days and hours and hours » a proof that the digital feeds were being intercepted and shared among the various insurgent groups* »[79]. Suite à l'opération militaire française Serval au Mali, le général Bernard Barrera dévoile également ce mode méconnu du grand public mais apprécié par les groupes armés. Selon lui, « *Les ordinateurs terroristes révèlent leurs secrets* ». Ils contiennent « *tous les cours imaginables du parfait terroriste : la manipulation d'explosifs, la décapitation d'êtres humains, des scènes de combat filmées…* »[80].

Pour ne pas mettre en péril l'organisation, les groupes armés prennent également leur précaution dans la communication vers leurs effecteurs. Ils dissimulent leurs flux informationnels grâce à la facilité de cryptage des données dans le cyberespace. Les outils numériques de communication présentent l'avantage d'être simples pour des personnes n'ayant pas de compétences particulières tout en étant terriblement puissants : « *Le grand public, et par voie de conséquence les voyous et les terroristes, dispose aujourd'hui des outils technologiques qui étaient jusqu'à ces dernières années réservés aux services de renseignement* »[81].

Dans la nébuleuse des groupes armés, un sympathisant de Daesh, Al-Khabir al-Taqni a même publié sur Internet la liste des moyens de communication cryptés les plus sûrs. La messagerie Telegram était notée comme "sûre" aux côtés de Wickr, Threema et Surespot. Il s'est félicité de cette capacité en affirmant : « *nous pouvons neutraliser l'une des armes les plus puissantes des gouvernement croisés pour espionner et suivre à la trace les moudjahidines, et les cibler avec des avions* »[82].

Pour atténuer au maximum leurs « empreintes numériques » et développer ainsi leur résilience, les groupes armés incluent également le « dark web »[83] dans leur stratégie digitale.

79 P.W. Singer et Allan Friedman, *op. cit.*, page 150
80 Général Bernard Barrera, *Opération Serval. Notes de guerre, Mali 2013*, Le Seuil.
81 http://www.lejdd.fr/Societe/Faits-divers/Terrorisme-Le-casse-tete-des-messageries-cryptees-743014, consulté le 05/12/2017.
82 https://tempsreel.nouvelobs.com/tech/20151120.OBS9921/telegram-wicker-ces-communications-cryptees-qui-echappent-a-toute-surveillance.html, consulté le 05/12/2017.
83 Réseau superposé à Internet utilisant des protocoles spécifiques pour anonymiser les utilisateurs. Aucun référencement de ce réseau n'est réalisé par les moteurs de recherche généralistes.

C'est une zone non référencée et inconnue de monsieur tout le monde. « *It has been described by The Economist as a dark corner of the Internet* »[84]. En téléchargeant des logiciels spécialisés populaires comme Tor, I2P ou Freenet, ils avancent masqués sur le dark web pour communiquaient et s'organisaient anonymement. « *C'est un véritable Far West virtuel »*[85]. Il devient alors très difficile de surveiller les flux et de les attribuer. « *L'inattribution est le cœur de la cyberstratégie. … Constatons qu'aujourd'hui l'inattribution est la règle. Surtout dans la lutte antique entre le glaive et le bouclier, toute tentative visant à démasquer les actions s'est vue immédiatement opposer des contre-mesures de camouflage* »[86]. Le darkweb est aujourd'hui au cœur de toute stratégie de camouflage. Daech contribue à démocratiser ce dernier en empruntant largement ses canaux pour « *toutes ses communications opérationnelles, ses collectes de dons et d'impôts révolutionnaires ou encore pour trafiquer en toute discrétion* »[87].

Certains groupes brouillent encore plus le tableau jusqu'à utiliser les jeux vidéo en ligne : « *En 2013, des documents confidentiels fournis par Edward Snowden avaient montré que la NSA et le GCHQ ont surveillé World of Warcraft pour tenter d'y déceler d'éventuels messages terroristes ou d'y trouver des groupuscules pour tenter de les infiltrer* »[88]. Cette innovation pour contourner la menace utilise :

- les possibilités de communication inter joueurs : « *la Playstation 4 serait exploitée pour communiquer vocalement via l'appli de voix sur IP intégrée au réseau PSN (PlayStation Network). D'après Jan Jambon, ces communications seraient plus difficiles à écouter que WhatsAp* »[89].
- de faire passer de courts messages à des complices via les actions dans le jeu en lui-même, par exemple : « *en écrivant sur un mur à l'aide de rafales d'armes au sein d'un jeu de tir. Ces messages sont quasiment indétectables et disparaissent rapidement* »[90].

84 P.W. Singer et Allan Friedman, *op. cit.*, page 108.
85 http://www.huffingtonpost.fr/jeremie-mani/daech-dark-web-reseaux-sociaux_b_8608220.html, consulté le 05/12/2017.
86 Olivier Kempf, *Introduction à la cyberstratégie*, Collection cyberstratégie, Economica, page 104.
87 http://www.huffingtonpost.fr, *ibid.* , consulté le 05/12/2017.
88 http://www.numerama.com/politique/226298-anti-terrorisme-la-france-surveille-de-pres-les-jeux-video-en-ligne.html, consulté le 03/12/2017.
89 https://www.francetvinfo.fr/replay-radio/nouveau-monde/reseaux-sociaux-messageries-jeu-video-comment-les-terroristes-communiquent_1790267.html, consulté le 05/12/2017.
90 http://www.numerama.com, *ibid.*, consulté le 03/12/2017.

Pour rendre encore plus difficile la mise en place de contre-mesures par les grandes armées étatiques, la stratégie numérique des groupes armés s'appuie sur des outils qui utilisent des infrastructures de communication qui ne leur appartiennent pas.

Si on cherchait à affaiblir une grande armée étatique, on pourrait s'en prendre à ses infrastructures de télécommunications, à ses systèmes d'informations et réseaux stratégiques de données qui constituent aujourd'hui ses « centres nerveux ». La cyberguerre vise principalement à neutraliser les infrastructures critiques du réseau adverse. Par contre pour affaiblir un groupe armé qui ne possède pas d'infrastructures propres, la capacité à affaiblir le dispositif cyber adverse est compromis. A part les terminaux numériques, il n'y a pas de point d'application réel pour une offensive. En effet, le cyberespace est essentiellement constitué d'éléments non militaires qui dépendent d'entreprises privées ou publiques : réseaux de téléphonie mobile, fournisseur d'accès à Internet, fibres optiques transocéaniques…. Ce ne sont pas des cibles légitimes au regard du droit des conflits armés, et les grandes armées étatiques ne peuvent détruire un réseau utilisé aussi bien par des acteurs publiques, privés, économiques et politiques... Les groupes armés deviennent inexpugnables.

2.8. Les outils de géolocalisation, compagnons indispensables aux groupes armés

Le GPS et les outils de géolocalisation associés (Google Earth, smartphone, applications avec « geotags »,...) sont de fidèles compagnons pour les groupes armés. Ils renforcent directement les piliers structurel et informationnel du modèle de résilience[91]. Ils leurs procurent liberté d'action et économie des forces. Que ce soit dans l'acquisition de renseignement, l'agilité et la discrétion, ces outils sont prisés car ils sont très accessibles et ne permettent pas d'être pistés.

Pour contourner la menace et s'attaquer au point le plus faible, les outils de géolocalisation s'avèrent efficace dans la planification des opérations. Ils leur procurent une source de renseignement des plus précises. Le quotidien britannique *The Telegraph* révèle que des cartes sur les implantations des unités militaires britanniques en Irak provenant de Google Earth ont été retrouvées dans des résidences terroristes irakiennes : « *We believe they use Google Earth to identify the most vulnerable areas such as tent* »[92].

91 Voir annexe.
92 http://www.telegraph.co.uk/news/worldnews/1539401/Terrorists-use-Google-maps-to-hit-UK-troops.html, consulté le 03/12/2017.

Dans *L'ensauvagement*, Thérèse Delpech évoque également l'utilisation d'un GPS par un groupe armé en plein cœur de l'Europe pour viser une « cible molle », une cible civile sans possibilité de riposte : « *même un pays comme la Suisse, où l'on se s'attendrait pas à trouver des indications de terrorisme non conventionnel, a trouvé dans le coffre d'une voiture arrêtée à la frontière pour un contrôle de routine, des détonateurs et un GPS comportant les coordonnées d'un réacteur de recherche nucléaire* »[93].

Les insurgés gagnent en autonomie et discrétion pour évoluer, se combiner et appliquer leur effort sur un point. Ils acquièrent une agilité dans la manœuvre d'attaque qui devient difficilement détectable. En Irak courant 2007, un groupe armé a réussi à localiser facilement une cible américaine, pourtant de nature militaire et dans un environnement sécurisé, sans être détectés : « *In 2007, US soldiers took smartphone photos of a group of new US Army helicopters parked at a base in Iraq and an then uploaded them to the Internet. …But the soldiers didn't realize the photos also included "geotags"… Insurgents then used these geotags to pinpoint and destroy four of the helicopters in a mortar attack* »[94].

La géolocalisation contribue également à effacer « leur empreinte au sol » et à les rendre indiscernables. En effet, forts de leur capacité de géolocaliser, ils développent des caches[95] pour leur soutien logistique (armes, véhicules, ravitaillement,...) et ne communiquent plus que de simples coordonnées aux membres d'un groupes ou autres groupes qui souhaitent se ravitailler. En 2015 autour de la passe de Salvador au Niger, l'armée française a mené une chasse à ses caches : « *en plein désert, au pied d'une dune, le capitaine Antoine se met à creuser dans le sable à un endroit très précis grâce aux photos satellites, aux coordonnées GPS et à son détecteur de métaux. … Un point de ravitaillement pour les pick-up* »[96].

93 Thérèse Delpech, *L'ensauvagement : Le retour de la barbarie au XXIe siècle*, Grasset.
94 Cybersecurity and cyberwar, P.W. Singer et Allan Friedman, Oxford University Press, page 102.
95 http://www.jeuneafrique.com/mag/426284/politique/sahel-piste-jihadistes-barkhane-traque-ag-ghaly-belmokhtar-autres/, consulté le 05/12/2018.
96 http://www.rfi.fr/afrique/20150421-reportage-barkhane-recherche-caches-jihadistes-desert-niger-armes-legionnaires, consulté le 02/12/2018.

2.9. L'impression 3D

Pour être encore plus résilient, les groupes armés s'intéressent également aux technologies émergentes pour le grand public comme l'impression 3D. Qualifiée comme « *Innovation technologique disruptive* »[97], cette dernière offre la capacité de fabriquer des armes ou pièces d'un système d'arme de manière autonome en dehors des filières classiques d'approvisionnement très surveillées. De plus, lorsque l'impression 3D est réalisée sur une base polymère, en plastique, elle devient indétectable au détecteur de métaux dans les aéroports, lieux publics... Sans numéros de série, une arme 3D est une arme « fantôme ». Un message posté sur un forum proche d'al-Qaïda vante les avantages de l'impression en 3D pour fabriquer des armes tout en *« appelant à s'emparer de cette méthode pour fabriquer des armes maison »*[98]. Cela peut devenir inquiétant lorsque l'on sait qu'« *une imprimante 3D comme la Replicator 2 fabriquée par la société MakerBot peut s'acheter par exemple pour 2 199 dollars, livrable en une semaine* »[99].

Cette technologie en plein essor offre des perspectives des plus intéressantes pour les groupes armés : « non-traçabilité des usages »[100] et « applications quasi infinies à venir » : pistolet, mines, pièces pour modifier des drones… Ce n'est pas de la science-fiction. Cette technologie a largement fait polémique il y a plusieurs années lorsque Cody Wilson, un étudiant américain en droit de 25 ans de l'Université du Texas, a réussi à imprimer entièrement un pistolet en plastique tout à fait fonctionnel, et surtout lorsqu'il a disséminé les plans sur Internet du premier pistolet 3D : « The Liberator ». Ses plans ont été téléchargés 100 000 fois en 2 jours avant d'être retirés par les autorités américaines[101].

La compréhension du renforcement de la résilience des petites organisations armés permet donc de mesurer à quel point le fossé se creuse sur ce point entre grandes armées étatiques et groupes terroristes. Cependant pour comprendre le pouvoir nivelant inattendu entre ces acteurs, la clé finale se trouve dans le caractère trompeur du « tout technologique » chez les grandes armées étatiques.

97 Asinetta Serban, livia Cahuzac-Soave et Axel Dyèvre, *Impression 3D – Des technologies de rupture au service des Armées*, Les notes stratégiques, juin 2016, CEIS ; page 8
98 http://m.france24.com/fr/20130329-site-djihad-3d-print-arme-impression-al-quaida-terrorisme-cody-wilson-fusil-assaut-technologie, consulté le 20/11/2017.
99 http://www.lemonde.fr/ameriques/article/2013/05/07/le-liberator-premier-pistolet-fabrique-avec-une-imprimante-3d-aux-etats-unis_3172075_3222.html, consulté le 24/11/2017.
100 Asinetta Serban, livia Cahuzac-Soave et Axel Dyèvre, *ibid.*, page 17.
101 https://www.theguardian.com/technology/2014/feb/10/cody-wilson-3d-gun-anarchist, consulté le 24/11/2017.

3. « L'atout trompeur »[102] des technologies pour les grandes armées étatiques au 21ième siècle

« *Si l'on se contente de l'opinion la plus répandue, la technologie constituerait l'atout décisif dans le combat* »[103]. Ce raccourci réducteur et néanmoins très populaire pourrait faire croire que les grandes armées étatiques au caractère technologique affirmé sont invincibles voire intouchables. Elles seraient les plus résilientes sans aucune comparaison. Au-delà de ce préjugé, la *revue stratégique de défense et de sécurité nationale 2017* de la France met en exergue que le détournement et la perte de contrôle des nouvelles technologies civiles et militaires atteint un niveau qui tend à niveler le rapport de force, et ce avec des acteurs de tout type, même insurrectionnels. Les plus résilients ne seraient pas forcément ceux à qui on pense en premier : « *Il n'y a pas de déterminisme technologique….La guerre relève plus de la théorie du chaos que du jeu d'échecs* »[104].

En effet, des petits groupes armés tendent bel et bien à obtenir une résilience supérieure à de grandes armées. Pourquoi ? Une partie de la réponse se trouve dans le fait que l'environnement technologique des armées de premier plan est sujet de plus en plus à « l'effet papillon ». Avec peu, on peut influencer grandement jusqu'à créer le chaos dans de grandes organisations. L'autre partie de la réponse est que les technologies ont rendu captives les grandes armées tout en générant un nombre important de failles techniques et humaines prêtes à être exploitées par ces adversaires.

3.1. La porte du chaos

L'incessante transformation technologique de notre société a touché tous les secteurs, du secteur primaire au secteur tertiaire en passant par les grandes armées étatiques. Un tsunami technologique a tout submergé. Aujourd'hui les grandes armées étatiques sont présentées technologiquement et opérationnellement supérieures grâce aux techniques de pointe. La technologie est au cœur des armées modernes, du soldat au centre de conduite des opérations, du sous-marin à l'avion de combat, de la tablette tactile embarquée dans un véhicule blindé au satellite… Un tissu technologique, un « nuage technologique » où les liens et les interdépendances constituent un système complexe…. et fragile.

---

102 JOZEFOWICZ, Henri, *Technologie : l'atout trompeur*, Défense et technologies, Cahiers Pensée mili-terre, numéro 48 – 3ième trimestre 2017, Centre de Doctrine et d'Enseignement du Commandement, page 3.

103 *Id.*

104 Centre de doctrine d'Emploi des Forces, *Des électrons et des hommes*, Cahier de la recherche doctrinale, 2005, page 44.

Sans détailler une par une les technologies et outils modernes, les derniers conflits (Irak, Afghanistan, Syrie,…), dans lesquels les armées occidentales ont été engagées, nous montrent que la technologie n'est pas l'atout décisif, et serait même la source d'une grande faiblesse. En effet, l'importance des interactions technologiques amènent aujourd'hui à ce qu'une infime variation de paramètre à un moment donné peut faire varier énormément le résultat final. Cela rejoint la théorie du chaos de Edward Norton Lorenz et sa métaphore du battement d'ailes d'un papillon[105].

Pour les grandes armées étatiques, le chaos peut survenir grâce à un « caporal stratégique », une faille informatique, une coupure électrique ou panne de climatisation mettant hors-service une salle serveur ou un nœud de communication rendant « sourd et aveugle » un théâtre d'opération ou une chaîne de commandement…. Dans Perspectives tactiques, le général Guy Hubin anticipait ce phénomène sur le thème du cyber : « *L'inoculation de virus, facilitée par la connexion des différents réseaux entre eux et par la compatibilité des différents systèmes, pourrait permettre de mettre en place au bon endroit les germes de la destruction de nombreux systèmes centraux, dont l'activation, déclenchée au moment opportun, pourrait paralyser des pans entiers des systèmes de commandement, d'acheminement de l'information, de navigation et de guidage. Il y a sûrement là de très intéressantes voies offensives à explorer, …*»[106]

3.2. Des géants aux pieds d'argile

Avions sans pilote, réseaux informatiques, satellites, supercalculateurs, lutte informatique offensive, la période post-11-septembre illustre l'ultra sophistication des grandes armées étatiques. « *Les pays riches, dont la France, ont fait le choix de la haute technologie pour construire leur appareil de défense. A vrai dire il n'y en avait pas d'autre possible* »[107]. Cependant cette intégration technologique à l'extrême semble ne pas les mettre à l'abri d'attaques ou de perturbations entamant leur résilience, ce qui peut paraître paradoxale. Dans une approche asymétrique, certains groupes armés n'hésitent pas à clamer *urbi et orbi* : « *Attention vous êtes encore plus vulnérables que nous ! Nous connaissons vos faiblesses !* ».

105 L'effet papillon fait qu'une cause minime puisse avoir des conséquences considérables.
106 Guy HUBIN, Perspectives tactiques, ECONOMICA, , page 84.
107 *Ibid.* , page 107.

« Techno-dépendants » et de plus en plus vulnérables au travers de leurs propres technologies, les grandes armées étatiques contribuent à émietter leur résilience tout en voyant se renforcer la résilience des groupes armés.

Un encerclement technologique

« *Confiant dans sa supériorité technologique et sa domination stratégique, le monde occidental a dimensionné son outil de défense au profit de la gestion efficiente de conflits limités reposant sur la neutralisation rapide des moyens de commandement adverses, les frappes de précision, le contrôle des lieux de décision.* »[108] Ce constat, tiré d'*Action Terrestre Future*, met en lumière cette sophistication des grandes armées étatiques. La technologie y est omniprésente pour frapper précisément, durement et avec « foudroyance ». Les grandes armées occidentales ont intégré de manière irréversible la technologie dans leur doctrine et leurs modes d'action. Cette dernière est omniprésente au point de parler de dépendance technologique.

Bombes guidées par GPS, réseaux informatiques,liaisons satellitaires, drones,... Les armées occidentales ont misé sur la technologie mais comme le souligne le général Vincent Desportes, alors commandant le Centre de Doctrine et d'Emploi des Forces, « *la technologie n'est plus un gage de supériorité ».* En effet, *«l a guerre de la coalition américano-britannique en Irak a montré que par l'utilisation des technologies les plus fines l'ennemi pouvait mettre en échec des armées bien équipées et largement numérisées* »[109]. Encerclée technologiquement, les grandes armées étatiques sont désormais captives de leurs outils et leurs doctrines. L'anticipation et l'identification de la menace asymétrique avec des modes d'action évanescents devient plus complexe et difficile.

« *En mars 2003, l'offensive américano-britannique sur l'Irak est le premier engagement réel de grande ampleur de forces richement dotées en nouvelles technologies de l'information* »[110]. La dépendance technologique a conduit à « *un étouffement des états-majors à partir de l'échelon brigade* »[111] avec des ordres qui « *n'ont jamais été aussi épais, aussi peu clairs et aussi tardifs* »[112].

108 Action terrestre future, 2017.
109 Asinetta Serban et Martin de Maupeou, *Rattrapages technologiques et technologie de l'information – La supériorité technologiques et opérationnelle des Armées au défi du numérique*, Les notes stratégiques, décembre 2015, CEIS, page26.
110 Centre de doctrine d'Emploi des Forces, *Des électrons et des hommes*, Cahier de la recherche doctrinale, 2005, page 37.
111 *Id.*
112 *Id.*

« *Des ordres d'opérations britanniques de brigades faisaient vingt-cinq pages, avec une mission qui n'apparaissait qu'à la dixième page* »[113]. Beaucoup d'ordres « *qui auraient pu être réduits à dix lignes faisaient trois ou quatre pages* ». Les états-majors les plus avancés du monde pour l'époque *« ont été finalement moins efficaces que ceux de 1944-45… Rappelons que lors de l'opération Market Garden, en septembre 1944, les Alliés ont été stoppés, et détruits à Amhem, par un corps d'armée blindée allemand qui avait reçu un ordre d'opérations de deux pages conçu et diffusé en quelques heures* ».[114]

Les plus vulnérables

En une phrase, le sénateur républicain américain McConnel synthétise la situation des grandes armées étatiques : « *we are the most vulnerable. We are the most connected. We have the most to lose* »[115]. En effet, le développement rapide des infrastructures numériques ne s'est pas toujours accompagné d'un effort parallèle de protection, et aujourd'hui les armées des pays riches se retrouvent avec des systèmes d'armes et de commandement largement numérisés et interconnectés qui augmentent considérablement leur vulnérabilité.

La dissémination et la sophistication des outils cybernétiques permettent de monter des cyberattaques avec des ressources limitées tout en provoquant des dommages importants. Ils donnent la possibilité d'atteindre facilement des réseaux ou des infrastructures critiques. « *La difficulté de contrôler la propagation des attaques, leurs vecteurs et leurs conséquences fait également courir des risques systémiques majeurs* »[116].

3.3. Retour de flammes

In fine, pour saisir comment les transformations numériques de la société et les dernières innovations technologiques ont permis aux petits groupes armés d'être plus résilients que de grandes armées étatiques, il faut comprendre que ces dernières peuvent être également dépassées par une intégration technologique qui impose un potentiel et un rythme « hors-limites » à des organisations caractérisée par une certaine inertie humaine et technique.

113 Centre de doctrine d'Emploi des Forces, *Des électrons et des hommes*, Cahier de la recherche doctrinale, 2005, page 37.
114 *Id.*
115 P.W. Singer et Allan Friedman, *op. cit.*, page 151.
116 Revue stratégique de défense et de sécurité nationale 2017, page 35.

Le facteur humain ou le maillon faible des grandes armées

Contrairement aux petits groupes, la dimension des grandes armées étatiques et le turnover associé de leurs unités nécessitent un effort constant de formation et d'entraînement, pilier essentiel de toute capacité. Sans formation ou entraînement récurrents pour maîtriser ces nouveaux outils, les technologies deviennent des freins à l'engagement dans les milieux très « abrasifs » des théâtres d'opérations militaires. Avec un manque de pragmatisme et de maîtrise, il est difficile d'exploiter les nouvelles technologies au maximum de leurs possibilités. « *A Sarajevo, en août 1993, une compagnie reçoit l'ordre de s'interposer entre les belligérants sur les Monts Igman. Le capitaine passionné d'informatique, entreprend de rédiger son ordre préparatoire par ordinateur. C'est un ordre magnifique mais il est donné lorsque les sections montent dans les VAB en direction des Monts Igman* »[117].

Plus difficiles à dépasser, les différences « idéologiques » existant entre les insurgés et les militaires représentent encore une source de faiblesse. Les nouveaux usages technologiques contribuent à modifier les modes de fonctionnement, les conditions et le cadre d'engagement des forces armées, mais aussi la vie quotidienne des militaires. A ce titre, les ressources humaines et leur adhésion aux technologies sont un enjeu structurant pour les armées quelques soient les générations. La sophistication des outils et la sensation de perte de contrôle peuvent effrayer surtout en présence de générations plus anciennes. Les « rétifs de principe », bien qu'en diminution, peuvent être un réel frein. « *L'épreuve du feu est souvent cruelle pour les nouvelles idées. Les premiers emplois de chars par les Britanniques en septembre 1916 et les Français, le 16 avril 1917 (76 engins détruits sur 121) sont désastreux. La première grande opération aéroportée alliée, en 1943 en Sicile, est un fiasco* »[118].

Dans un monde en perpétuel changement, la technologie demeure un facteur de progrès évident. Elle innerve des niveaux les plus hauts aux niveaux les plus bas. Quelques fois, elle est à l'origine d'un manque d'homogénéité dans l'ambition de l'utilisation des outils « dernier cri ». Ainsi, les drones de combat présentés comme l'avenir des armées du monde laissent apparaître des difficultés avec des pilotes de drones qui perdent pied avec la réalité.

117 Des électrons et des hommes, Cahier de la recherche doctrinale, Centre de doctrine d'Emploi des Forces, 2005, page 26
118 *Ibid.*, page 11

Le *New York Times* rappelle qu'un rapport du Pentagone, en 2013, avait montré que les pilotes de drones subissaient les mêmes pressions psychologiques que les pilotes d'avions de guerre, et certains arrivent au «burn-out » dû au décalage trop important entre le virtuel, leur écran tel un jeu vidéo, et la réalité des combats[119]. Aux Etats-Unis, les affaires Snowden ou Bradley Manning montrent également qu'un seul maillon faible dans une chaîne hautement numérisée peut briser un système jugé résilient et intouchable. Ce phénomène de « caporal stratégique » prend une dimension hors-limites dans la perte de résilience lorsque des technologies puissantes sont confiées à des individus qui s'écartent de l'ambition collective d'une organisation.

Des failles dans la cuirasse des grandes armées

Dans un contexte d'intégration technologique croissante, les nouveaux outils technologies présentent de formidables opportunités, ils constituent dans le même temps de nouveaux défis. Refuser ses défis et donc le changement, rester sur des positions ou s'attarder sur des technologies peut amener vers un système sclérosé, un outil émoussé où des années d'attentisme peuvent se transformer en décennies de retard.

En effet, une autre cause pour comprendre la plus grande résilience des petits groupes par rapport aux grandes armées étatiques est leur attrait et utilisation immédiate des nouvelles capacités si elles peuvent servir leur cause, au grand damne des grandes armées étatiques souvent dans l'attente pour observer et analyser les retours d'expérience des dernières avancées. Cet attentisme voire défiance peut ainsi émietter la résilience des grandes armées. En 2012, le sénateur Jean-Marie Bockel a dressé un bilan inquiétant sur le dispositif de cyberdéfense français. Dans son rapport *La cyberdéfense : un enjeu mondial, une priorité nationale*[120], il évoque « *des alliés mieux armés* », et « *un dispositif qui connait encore d'importantes lacunes* ». A l'instar du mouvement cyber planétaire, l'armée française avait commencé avec un retard significatif.

De plus, en quelques décennies, les grandes armées étatiques sont passées d'un rôle de leader à suiveur dans presque toutes les grandes révolutions technologiques. Le temps d'avance sur un adversaire pour frapper rapidement, par surprise ou encore se défendre s'est drastiquement réduit.

119 http://www.lemonde.fr/international/article/2015/06/17/le-burn-out-des-pilotes-de-drone-de-l-armee-americaine_4656252_3210.html#pVPBbsIhyudLtyQc.99, consulté le 11/12/2017.
120 Rapport d'information de M. Jean-Marie BOCKEL, fait au nom de la commission des affaires étrangères, de la défense et des forces armées n° 681 (2011-2012) - 18 juillet 2012.

Un rendement décroissant est même souligné dans la *Revue stratégique de défense et de sécurité nationale 2017* :« *une quinzaine d'experts font part de leurs inquiétudes. Historiquement, les ruptures majeures en matière d'armement ont été le fruit de financements à finalité militaire, mais aujourd'hui, le domaine civil fait émerger un nombre croissant de technologies d'intérêt militaire* »[121]. Les militaires n'ont plus l'exclusivité de l'innovation majeure. Grâce à cette nouvelle forme de dissémination technologique, des individus ou groupes peuvent se doter de « *capacités jusqu'ici maîtrisées par un nombre restreint d'États* »[122], et bénéficier d'une plus grande résilience.

La maîtrise de la haute technologie est une condition nécessaire aux grandes armées pour maintenir leur puissance et résilience mais elles sont dépendantes de leurs industries de défense pour garder ce niveau. Hors les évolutions technologiques duales et leur multiplication « *fragilisent leurs industries de défense* »[123]. Ces dernières sont poussées hors de certains domaines technologiques par des acteurs civils de plus en plus actifs. Un risque de décrochage technologique est réel et entraîne des failles dans la cuirasse de grandes armées étatiques.

Sans industries de défense performantes, les militaires peuvent se voir reprocher de préparer que la guerre d'hier ou d'aujourd'hui et jamais celle de demain. Ainsi dans le renseignement, de grandes armées occidentales ne se sont pas organisées efficacement avec leur industrie de défense pour rester à la pointe du big data et faire face au défi de la surinformation. Aujourd'hui, les informations sur Internet sont noyées dans des myriades de données. « *Chaque minute, 350 000 messages sont ainsi envoyés sur Twitter, 3 millions de vidéos visionnionnées sur Youtube ; 200 millions de mails échangés entre ordinateurs* »[124]… Le général Hubin avait discerné cette faiblesse : « *La difficulté ne sera plus tant d'acquérir l'information, mais de la gérer convenablement, ... Les problèmes ne seront plus le résultat de l'ignorance, mais plutôt du trop plein* »[125].

* *

*

121 Guerric Poncet, *Le salut des armées passera par l'ultra high-tech et le cyber*, Le Point, 17/10/2017
122 Revue stratégique de défense et de sécurité nationale 2017, page 33
123 *Id.*
124 Science et guerre - nouveaux conflits, nouvelles technologies, Hors-série n°182, juil-août 2015, Sciences et avenir.
125 Guy HUBIN, *op. cit.* , page 107.

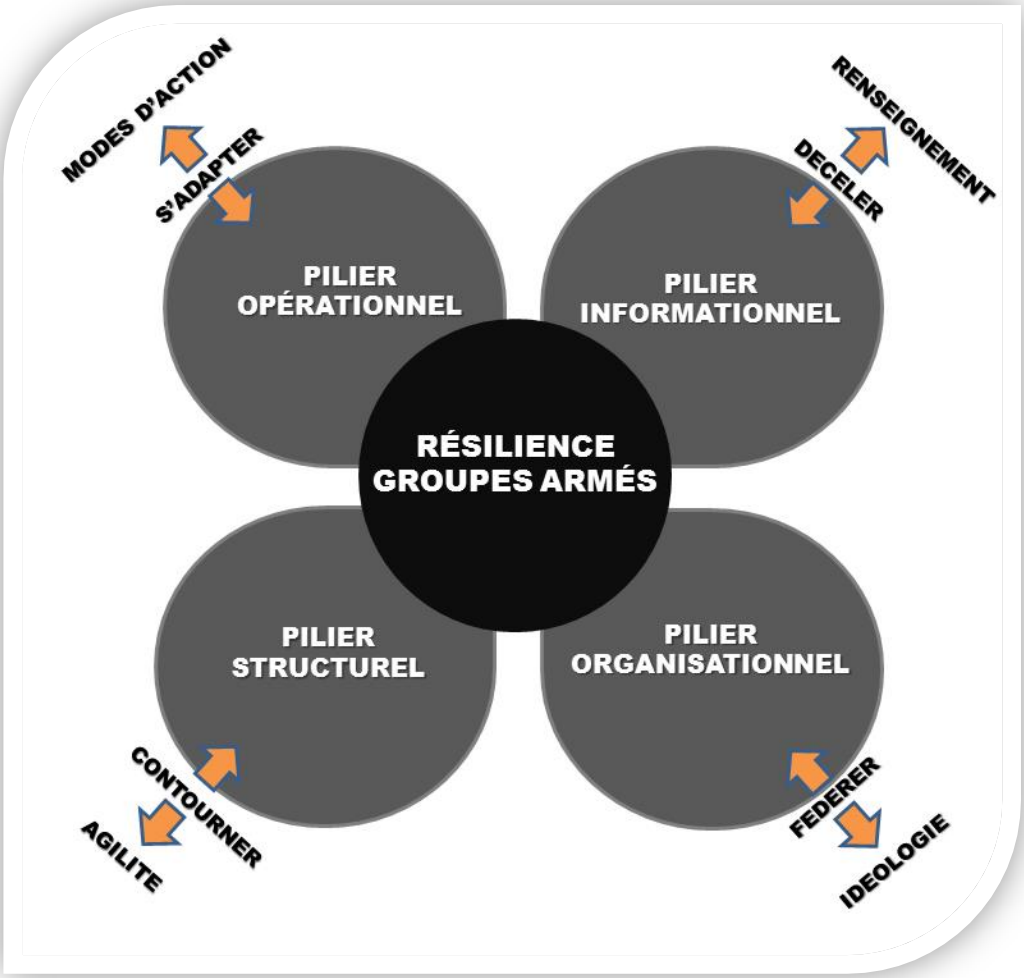
En dépit des dernières avancées numériques et techniques de la société occidentale qui constituent le facteur déterminant de la supériorité technologique et opérationnelle des grandes armées étatiques, la prolifération et dissémination des technologies modernes souvent d'intérêt militaire permettent à des individus et groupes pratiquants une insurrection armée (terroristes, groupes armés paramilitaires) de trouver une source de résilience « hors-limites » et préoccupante. Des adversaires asymétriques peuvent ponctuellement devenir invulnérables, du moins capable de neutraliser l'avantage du fort.

La transformation numérique de la société et la globalisation des technologies récentes génèrent et alimentent un nouvel ordre sur l'échiquier planétaire. La guerre « hors limites » prédite par les colonels chinois Qiao Liang et Wang Xiandsui avec la globalisation des technologies offre un potentiel et un rythme sans limites. Des acteurs insurrectionnels, autrefois voués à disparaître, trouvent dans les nouvelles technologies une source de résilience considérable. Les nouvelles technologies leurs permettent de s'adapter à leur environnement et de s'y fondre tel le caméléon. A l'instar de la pieuvre, elles les autorisent également à développer un réseau tentaculaire agile et résistant, et elles leur confèrent une faculté de résurgence tel le phénix. Cette dynamique est renforcée par l'atout trompeur que les technologies présentent aux grandes armées pensant être invincibles, et sûres de leur pouvoir de terrasser un adversaire insignifiant au regard de leur taille et capacité opérationnelle.

Il n'y a pas de déterminisme technologique. Cependant, le monopole de l'usage de la force « ultra high-tech » combinée à la méthode optimale d'utilisation semble être la meilleure des réponses de la part des grandes armées étatiques appuyées par leurs industries de défense. Dans *Perspectives tactiques*, le général Guy HUBIN anticipe cette option : « *Au bout du compte nos adversaires éventuels posséderont certainement les matériels et probablement les logiciels du même niveau que les nôtres, mais ce qu'ils ne maîtriseront peut-être pas c'est la méthode optimale d'utilisation, car elle promet d'être extraordinairement complexe* »[126]. De la capacité des grandes armées étatiques à maintenir au plus haut la maîtrise technologique etleur audace pourraient dépendre demain l'ordre ou le désordre du monde.

126 Guy HUBIN, *op. cit.* , page 86.

ANNEXE



Piliers conceptuels de la résilience des groupes armés.

SOURCES ET BIBLIOGRAPHIE

Ouvrages

- Bertrand BOYER, *Cybertactique Conduire la guerre numérique*, Nuvis.
- Qiao Liang, Wang Xiandsui , *La guerre hors limites*, Rivages poche.
- David Galula, *Contre-insurrection Théorie et pratique*, Economica.
- Maréchal Ferdinand Foch, *Des principes de la guerre*.
- Sous la direction d'Olivier Entraygues, *L'âge du drone*, Polémoscopie n°2, Le Polémarque.
- P.W. Singer et Allan Friedman, *Cybersecurity and cyberwar*, Oxford University Press.
- Général Bernard Barrera, *Opération Serval. Notes de guerre*, Mali 2013, Le Seuil.
- Olivier Kempf, *Introduction à la cyberstratégie*, Collection cyberstratégie, Economica.
- Thérèse Delpech, *L'ensauvagement : Le retour de la barbarie au XXIe siècle*, Grasset.
- Guy HUBIN, *Perspectives tactiques*, ECONOMICA.

Documentations et ouvrages institutionnels

- *Livre blanc sur la défense et la sécurité nationale* de 2013.
- Centre interarmées de concepts, de doctrines et d'expérimentations, C*oncept d'emploi des forces.*
- *(CEF)*, CIA –0, Concept interarmées N° 004/DEF/CICDE/NP du 11 janvier 2010.
- Monsieur le sénateur Bruno SIDO et monsieur le député Jean-Yves LE DÉAUT, fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, *Les drones et la sécurité des installations nucléaires*, Rapport n° 267 (2014-2015) du Sénat, , déposé le 29 janvier 2015, Introduction.
- Réflexion doctrinale interarmées, *Réseaux sociaux, Nature et conséquences pour les forces armées*, RDIA-2013/001 RS(2013), N° 067/DEF/CICDE/NP du 19 avril 2013.
- M. Jean-Yves Le Drian, Ministre de la défense, *discours d'ouverture du colloque sur la cyberdéfense*, Rennes, 3 juin 2013.
- *Revue stratégique de défense et de sécurité nationale 2017*, publié le 13 octobre 2017.
- Directions des affaires stratégiques, *horizons stratégiques*, 2012.
- Centre de doctrine d'Emploi des Forces, *Des électrons et des hommes*, Cahier de la recherche doctrinale, 2005.
- *Action terrestre future*, 2017.
- JOZEFOWICZ, Henri, *Technologie : l'atout trompeur*, Défense et technologies, Cahiers Pensée mili-terre, numéro 48 – 3ième trimestre 2017, Centre de Doctrine et d'Enseignement du Commandement.
- Rapport d'information de M. Jean-Marie BOCKEL, fait au nom de la commission des affaires étrangères, de la défense et des forces armées n° 681 (2011-2012) - 18 juillet 2012.

Articles de presse contemporains

- Dorothée Kohler, Jean-Daniel Weisz, *La France doit s'inspirer du projet « Industrie 4.0 » allemand*, Le Monde, 14/11/2014.
- GUERRIC PONCET, *Le salut des armées passera par l'ultra high-tech et le cyber*, Le point, 17/10/2017.
- Mohammad-Mahmoud Ould Mohamedou, interview du journaliste Frédéric Koller, Le Temps, 26 juillet 2016.
- Nathalie Guibert, *Paris veut sortir « Barkhane » du piège malien*, Le Monde, le 15/11/2017.

- Etienne Dubuis, *Les drones miniatures, une nouvelle arme aux mains des terroristes*, Le Temps, 9/03/2015.
- Jean-Michel Normand, *Le drone de loisir, nouvelle arme du terrorisme ?,* Le Monde, 11/10/2016.
- Guerric Poncet, *Une frégate saoudienne frappée par un drone naval houthi*, Le point, 23/02/2017.
- Judikael Hirel, *Syrie : l'EI conquiert une base grâce à un drone à 450 euros*, Le Point, 31/08/2014.
- AFP, *Les drones de l'EI inquiètent l'Occident*, La tribune de Genève, 3/03/2017
- Christophe Lamfalussy, *Un atelier de drones de Daech découvert en Irak*, La libre Belgique, 19/10/2016.
- Guerric Poncet, *Le salut des armées passera par l'ultra high-tech et le cyber*, Le Point, 17/10/2017
- Nathalie Guibert, *Cyberattaques : l'armée a activé pour la première fois une cellule de crise*, Le Monde, 17/01/2015.
- AFP, *Le compte Twitter de l'armée américaine piraté par l'État islamique*, Le Point, 12/01/2015.
- Sous la direction de Flore de Feydeau , *Espace numérique, Un nouveau champ de bataille*, Armées d'aujourd'hui n° 415 Avril 2017, page 22.
- Science et guerre - nouveaux conflits, *nouvelles technologies*, Hors-série n°182, juil-août 2015, Sciences et avenir.
- Asinetta Serban, livia Cahuzac-Soave et Axel Dyèvre, I*mpression 3D – Des technologies de rupture au service des Armées*, Les notes stratégiques, juin 2016, CEIS.
- Asinetta Serban et Martin de Maupeou, *Rattrapages technologiques et technologie de l'information – La supériorité technologiques et opérationnelle des Armées au défi du numérique*, Les notes stratégiques, décembre 2015, CEIS.
- Alix Desforges , *Les représentations du cyberespace : un outil géopolitique, Hérodote, Cyberespace : enjeux géopolitiques*, 2014/1 (n° 152-153).
- Stéphane Dossé, Olivier Kempf, *Stratégies dans le cyberespace*, cahier de l'AGS N°2, L'esprit du livre, 2011.
- Colonel Vincent Gelez, *Les canaux de la confiance. La résilience des petits groupes,* Revue inflexions, n° 29, 2015.

Sites Internet

- http://www.mbadmb.com/2016/12/11/societe-4-0/, consulté le 16/01/2016
- http://robots.blog.lemonde.fr/2016/11/15/un-peu-plus-dinfos-sur-les-drones-de-letat-islamique/, consulté le 11/11/2017.
- http://www.lefigaro.fr/flash-actu/2017/01/31/97001-20170131FILWWW00261-les-drones-tueurs-de-l-ei-de-plus-en-plus-efficaces.php, consulté le 31/01/2018.
- http://www.lefigaro.fr/secteur/high-tech/2018/01/29/32001-20180129ARTFIG00212-une-application-de-fitness-devoile-la-position-de-bases-militaires-secretes.php, consulté le 31/01/2018.
- http://www.lefigaro.fr/international/2017/01/08/01003-20170108ARTFIG00050-le-ministere-de-la-defense-a-dejoue-24000-cyberattaques-en-2016.php, consulté le 02/12/2017.
- http://www.geopolitique.net/fr/lutilisation-dinternet-et-des-reseaux-sociaux-lors-de-loperation-militaire-israelienne-a-gaza-en-novembre-2012/, consulté le 04/12/2017.
- http://www.opex360.com/2012/11/19/pilier-de-defense-israel-est-la-cible-de-millions-de-cyberattaques/, consulté le 04/12/2017.
- https://www.francetvinfo.fr/monde/un-groupe-se-reclamant-de-daech-publie-des-donnees-confidentielles-de-l-armee-us_1681179.html, consulté le 04/12/2017.
- http://www.lejdd.fr/Societe/Faits-divers/Terrorisme-Le-casse-tete-des-messageries-cryptees-743014,

consulté le 05/12/2017.
- https://tempsreel.nouvelobs.com/tech/20151120.OBS9921/telegram-wicker-ces-communications-cryptees-qui-echappent-a-toute-surveillance.html, consulté le 05/12/2017.
- Opex360.Com - 09 avril 2015 - Via une cyberattaque d'ampleur inédite contre TV5 Monde, l'État islamique menace les familles des militaires français, consulté le 04/12/2017.
- http://www.huffingtonpost.fr/jeremie-mani/daech-dark-web-reseaux-sociaux_b_8608220.html, consulté le 05/12/2017.
- http://www.huffingtonpost.fr, ibid. , consulté le 05/12/2017.
- http://www.numerama.com/politique/226298-anti-terrorisme-la-france-surveille-de-pres-les-jeux-video-en-ligne.html, consulté le 03/12/2017.
- https://www.francetvinfo.fr/replay-radio/nouveau-monde/reseaux-sociaux-messageries-jeu-video-comment-les-terroristes-communiquent_1790267.html, consulté le 05/12/2017.
- http://www.telegraph.co.uk/news/worldnews/1539401/Terrorists-use-Google-maps-to-hit-UK-troops.html, consulté le 03/12/2017.
- http://www.jeuneafrique.com/mag/426284/politique/sahel-piste-jihadistes-barkhane-traque-ag-ghaly-belmokhtar-autres/, consulté le 05/12/2018.
- http://www.rfi.fr/afrique/20150421-reportage-barkhane-recherche-caches-jihadistes-desert-niger-armes-legionnaires, consulté le 02/12/2018.
- http://m.france24.com/fr/20130329-site-djihad-3d-print-arme-impression-al-quaida-terrorisme-cody-wilson-fusil-assaut-technologie, consulté le 20/11/2017.
- http://www.lemonde.fr/ameriques/article/2013/05/07/le-liberator-premier-pistolet-fabrique-avec-une-imprimante-3d-aux-etats-unis_3172075_3222.html, consulté le 24/11/2017.
- https://www.theguardian.com/technology/2014/feb/10/cody-wilson-3d-gun-anarchist, consulté le 24/11/2017.
- http://www.lemonde.fr/international/article/2015/06/17/le-burn-out-des-pilotes-de-drone-de-l-armee-americaine_4656252_3210.html#pVPBbsIhyudLtyQc.99, consulté le 11/12/2017.