Bertrand Boyer

Guérilla 2.0

Guerres irrégulières dans le cyberespace

Préface du général d'armée
Thierry Burkhard
Chef d'état-major de l'armée de Terre

ligne de front

Guérilla 2.0

Bertrand Boyer

Guérilla 2.0

Guerres irrégulières dans le cyberespace

Préface du général d'armée
Thierry Burkhard
Chef d'état-major de l'armée de Terre

éditions de l'école de guerre

Collection
Ligne de front

Note de l'éditeur

L'École de guerre est un lieu d'étude et de réflexion où se forment les chefs de demain : ceux de la prochaine guerre de Troie, de cent, de trente ou de sept ans… Mais nos combats ne se mènent plus dans la lice, entre les palissades d'un terrain clos. Ils ne concernent pas seulement les militaires dévoués à leur pays, quelques mercenaires égarés ou les enfants perdus de tristes tropiques. Ils sont une responsabilité collective de nos démocraties. L'étude et la réflexion ne peuvent être le seul fait d'officiers développant leur pensée dans ce quadrilatère hors du temps que serait l'École militaire si elle ne s'ouvrait sur le monde.

Là réside la vocation des Éditions de l'École de guerre : susciter l'intelligence, encourager l'écriture et publier au profit de la réflexion et du dialogue de tous, civils ou militaires.

Cette maison d'édition ne diffuse pas la *doxa* officielle qui a pour s'exprimer d'autres organes. Elle ne représente pas même les doctrines de l'École de guerre. Elle souhaite simplement rendre publics des ouvrages qui, polémiques ou non, n'engagent que leurs auteurs

mais contribueront à la pensée militaire, géopolitique et stratégique française.

Elle repose pour cela sur six collections :

– la collection « Champs de bataille » traite d'histoire, de géopolitique et de stratégie ;

– la collection « Ligne de front » illustre cette nécessité de « penser autrement » qui est l'un des *leitmotivs* de l'École de guerre ;

– la collection « Feux croisés » aborde des réalités et des problématiques parallèles ou au contraire divergentes ;

– la collection « Honni soit qui mal y pense » publie en langue anglaise des textes porteurs d'une certaine pensée française ;

– la collection « Citadelle » réédite des grands textes de la littérature militaire ;

– la collection « Quartier libre » est une école buissonnière dans le monde des armes ou à ses frontières.

Avertissement

Dans le prolongement des réflexions engagées dans *Cyberstratégie, l'art de la guerre numérique* (2012), et *Cybertactique, conduire la guerre numérique* (2014) cet ouvrage interroge l'évolution des mécanismes insurrectionnels et terroristes à l'ère numérique.

Il s'agit ici de poursuivre l'étude de la conflictualité dans le cyberespace en cherchant à comprendre les liens entre technique et tactique, stratégie générale et stratégie opérationnelle : comment les guérillas utilisent le cyber ? Y a-t-il place pour un combat spécifique nécessitant de revisiter certaines habitudes ? Le cyberespace bouleverse-t-il les modes de guerre ? Enfin, alors que les études et les théories sur la contre-insurrection se sont développées à la fin du XX^e^ siècle, quelles leçons pouvons-nous en tirer dans le cadre du combat numérique ?

Fruit d'une réflexion personnelle et de plusieurs années de pratique dans le domaine de la cyberdéfense et des opérations, les idées exposées n'engagent que l'auteur et ne constituent pas le point de vue officiel du ministère des Armées.

Ainsi, les principes, modèles et illustrations qui seront développés au long de ces lignes n'ont aucune valeur officielle et ne représentent pas les choix des autorités civiles ou militaires. Ils ne sont qu'une contribution personnelle aux débats et recherches académiques actuels et n'ont d'autre ambition que de provoquer la réflexion.

Les descriptions techniques sont quasi absentes de ce traité, elles seront limitées au strict minimum et ne serviront que d'illustrations aux thèses développées. L'approche de l'auteur repose sur la conviction qu'une réponse ne peut être trouvée qu'en intégrant de multiples disciplines et en croisant les expériences. Privilégiant donc la synthèse et l'interdisciplinarité, certains concepts ne sont qu'abordés succinctement, d'autres plus longuement ; non qu'ils soient plus importants, mais il nous a semblé que leur valeur d'illustration était plus importante. Le spécialiste trouvera donc probablement dans cet ouvrage des raccourcis qui lui sembleront inacceptables, voire des erreurs pour lesquelles il voudra bien excuser l'auteur. L'historien y relèvera certainement des erreurs ou des approximations, dont il faut souhaiter qu'elles ne nuisent pas à l'argumentation.

En évitant les comparaisons, toujours délicates, sans pour autant les supprimer totalement, la démarche privilégie l'interrogation des concepts par le retour à la théorie. On pourra ainsi reprocher la longueur de certains développements historiques. Il a pourtant paru essentiel de replacer le combat numérique et particulièrement

celui de la guérilla dans une perspective plus large, afin notamment d'éviter une forme d'éblouissement de la modernité.

Préface

La révolution dans les technologies de l'information et de la communication engagée à la fin du XX^e siècle a entraîné une transformation majeure de notre société. Des changements profonds innervent les moindres aspects de nos vies à une vitesse qui laisse peu de temps pour en mesurer toutes les conséquences. L'éducation, l'économie, la culture, la politique, les loisirs et bien évidemment la défense entrent dans le nouvel âge de l'ère numérique. En moins de trente ans, la maîtrise de l'information est devenue un enjeu stratégique.

De ce monde interconnecté, rendant possible l'utopie d'une société totalement ouverte et transparente, de nouvelles menaces ont émergé. Elles profitent de notre besoin accru d'échanger et exploitent les vulnérabilités de nos systèmes. Ces menaces sont à la fois difficilement prévisibles et en évolution permanente. Elles ont un impact de plus en plus sévère, y compris en opérations. Les comprendre, à défaut de les anticiper réellement, constitue la première étape de la réflexion qui doit nous permettre d'adapter notre outil de défense.

C'est ce que nous propose avec pertinence le livre du colonel Bertrand Boyer.

Il y a encore peu de temps, la cyberguerre n'était imaginée que sous son visage le plus critique, l'équivalent d'un Pearl Harbor informatique capable de mettre à genoux une société entière par la diffusion d'un simple virus informatique qui désorganiserait l'ensemble de nos réseaux. S'il ne faut pas écarter cette hypothèse, l'éventail des actions dans le cyberespace est bien plus large. Œuvre d'acteurs étatiques ou infra-étatiques, les actions numériques paraissent bien plus insidieuses et leur attribution est rendue de plus en plus difficile. Elles permettent l'endoctrinement et le recrutement de terroristes, la mobilisation de mouvances radicales *via* les réseaux sociaux, le vol de données informatiques ou la diffusion massive de fausses informations visant à briser la cohérence des sociétés occidentales.

Nous pensions la stratégie numérique suivant une approche directe. Mais nous oublions que nos adversaires ont de plus en plus recours à l'approche indirecte qui mêle guerre de l'information, opérations clandestines, combats conventionnels ou actions terroristes. Ils cherchent, y compris dans le cyberespace, à nous affaiblir dans la durée et à imposer leur volonté. Nous sommes dès lors confrontés à ce que le colonel Bertrand Boyer appelle à juste titre de la cyber-guérilla. Cette guérilla 2.0 ne se substitue pas aux modes d'actions guerriers ou contestataires traditionnels, elle les complète et ouvre un nouveau champ de conflictualité pour les armées modernes.

Les principes de la guerre ne changent pas mais de nouvelles armes sont désormais à disposition des organisations extrémistes violentes tandis que davantage d'États cherchent à imposer leur volonté. Les conflits se transforment, non dans leur essence mais dans les modalités d'affrontement des adversaires qui se retrouvent de plus en plus à égalité technologique.

Toute la force de cet ouvrage est qu'il propose une réflexion de stratège et de tacticien, en faisant des allers-retours permanents entre les champs physiques et les champs immatériels pour mieux en démontrer les similitudes. Le colonel Bertrand Boyer invite plus que jamais nos armées à penser le cyberespace comme un nouveau milieu de confrontation où doivent s'appliquer les principes de la guerre que nous connaissons.

C'est un enjeu majeur pour l'armée de terre qui doit tout d'abord renforcer la résilience de nos hommes et de nos états-majors au travers d'une nouvelle forme de « techno rusticité » pour protéger notre chaîne de commandement et nos processus décisionnels désormais vulnérables à cette guérilla 2.0.

Ce sont également nos équipements qu'il convient de durcir contre les diverses agressions cyber et électroniques. Le combat de haute intensité se caractérise d'abord par la perte relative de supériorité dans des domaines où nous n'étions pas, jusqu'alors, contestés.

Enfin, l'armée de terre doit développer de nouvelles capacités d'attaque avec des moyens et des doctrines adaptés. Au-delà des actions classiques et cinétiques,

soyons désormais capables de combiner nos effets avec le cyberespace et le champ informationnel.

La tactique ne peut plus être cantonnée au seul champ physique. Nous devons aussi savoir manœuvrer dans les champs immatériels, seul moyen de déployer une véritable stratégie de contre-guérilla 2.0 et de vaincre nos adversaires.

Général d'armée Thierry Burkhard
Chef d'état-major de l'armée de Terre

À nos sentinelles numériques

Introduction

« Va-t'en, chétif insecte, excrément de la terre ! » Voici les premiers mots que prononce le lion attaqué par le moucheron dans la fable de Jean de La Fontaine. Ce dernier est un auteur rarement étudié en stratégie, pourtant sa fable du lion et du moucheron illustre parfaitement la permanence du combat qui oppose le faible au fort, combat asymétrique dirions-nous aujourd'hui. Cette métaphore, présente dans les textes sacrés des principales religions monothéistes[1], amène à s'interroger sur la pertinence et la permanence de cette forme d'affrontement à l'ère numérique. L'asymétrie qui caractérise le combat insurrectionnel connaît dans le cyberespace un développement particulier. Le combat irrégulier n'est plus aujourd'hui limité dans son arsenal tant les outils numériques lui sont aisément accessibles. Ainsi, si la guérilla est aussi vieille que la guerre elle-même, quelles modifications pouvons-nous en attendre dans le contexte de numérisation croissante des armées ?

1. Un épisode de la Bible relate le combat de David contre Goliath (Samuel 17, 1-58) durant lequel le jeune berger vient à bout du géant philistin à l'aide d'une fronde. Un épisode similaire est présent dans le Coran (al-baqarah verset 251).

Alors même que les nouvelles technologies favorisent le développement d'une société plus ouverte, interconnectée, où les échanges économiques et culturels sont facilités, elles permettent également l'émergence de nouvelles menaces. Les formes de gouvernement classiques sont fragilisées par la prolifération des outils numériques et les anciens ordres sont plus directement remis en cause. Les acteurs de la scène internationale ont changé, et ce mouvement paraît irréversible. Des multinationales qui ne produisent rien mais qui « connectent » des usagers font évoluer notre rapport au travail, à la vie privée, aux services.

La nature des conflits et des engagements militaires s'en trouve ainsi modifiée, non dans son essence, puisqu'il s'agit toujours d'imposer par la force sa volonté à un adversaire, mais dans sa matérialisation et sa réalisation. En la matière, il convient de ne pas oublier les leçons de l'histoire. Celle-ci nous enseigne que les évolutions technologiques n'effacent pas les modes d'actions antérieurs : elles les complètent, les modifient et en ajoutent de nouveaux. Ainsi, l'augmentation observée des engagements contre des acteurs non-étatiques ne signifie pas pour autant la fin des affrontements de grandes forces conventionnelles. Il n'est qu'à constater les augmentations de dépenses militaires dans le monde pour se convaincre que cette menace n'est pas un scénario improbable. L'outil de défense est donc contraint entre la réalité des engagements asymétriques contre des groupes armés terroristes et le maintien d'un

rapport de force classique garantissant la sécurité et l'intégrité des territoires.

Ce paradoxe est au cœur des politiques de défense et de sécurité. Il faut anticiper de nouvelles menaces et s'adapter, sans sacrifier à l'existant ni s'engager dans des choix qui impliqueraient des abandons capacitaires. Ces mutations imposées aux armées par un adversaire au visage changeant, que certains appellent « hybride », ne sont que la face visible des évolutions en cours. Il est ainsi très probable que les doctrines, modèles d'organisation et de fonctionnement actuels, héritées d'une continuité historique dans la manière d'aborder les formes de conflits et l'ennemi, ne résistent pas à « l'uberisation » de l'adversaire. Notre premier devoir est de penser ces changements à défaut de pouvoir totalement les anticiper.

Dans ce contexte, les espaces numériques sont un champ de développement rapide pour les études stratégiques et tactiques. Ils constituent un puissant vecteur, tant pour diffuser des idées ou des informations, que pour conduire des actions plus agressives sur les systèmes d'information. L'abaissement des coûts d'entrée pour accéder à certaines technologies autrefois réservées aux services étatiques tels que le chiffrement, la production et la diffusion de produits de propagande ou encore des outils d'intrusion, permet à des acteurs, autrefois mineurs, de faire peser une menace accrue. Si l'émergence du cyberespace comme un champ d'affrontement à part entière ne fait aujourd'hui plus débat,

il nous revient d'anticiper la forme que prendront ces affrontements.

Les premières réflexions sur ces questions remontent aux débuts des années 1990, avant même le développement de l'Internet et concomitamment à l'invention du Web par Tim Berners-Lee et les chercheurs du CERN. Pendant près de vingt ans, c'est avant tout une vision « apocalyptique » qui l'emporte, les cyberattaques sont d'abord envisagées sous l'angle d'un pouvoir destructeur à une échelle qui égalerait celle de l'arme nucléaire. Les scénarios prospectifs se rapprochent alors de la science-fiction, laissant entendre que d'un clic un attaquant pourrait neutraliser la production électrique d'un pays, le plonger dans le chaos en paralysant les centres de décisions et de production. Cette forme de *Blitzkrieg* numérique, tout en demeurant une hypothèse de probabilité non nulle (au même titre qu'une frappe nucléaire unilatérale sur des villes), semble pourtant très éloignée de la réalité des affrontements observés dans le cyberespace.

Alors que l'on s'attendait à ce que les outils numériques rejoignent le panthéon des armes de destruction massives, la quête de l'*ultima ratio* a masqué les développements rapides des autres formes de combats numériques. Ainsi, si potentiel de destruction il y a, celui-ci est très largement limité par la nature même des réseaux (localement fragiles, globalement résilients). Loin d'être un espace « lisse », le cyberespace est un écheveau de réseaux compartimentés, divisé en zones, segmenté par les applications, régulé par des protocoles.

Cet aspect engendre nécessairement des frictions qui conduisent des auteurs comme Laurent Henninger à qualifier cet espace de fluide [Henninger, 2012]. La capacité destructrice d'une arme numérique est donc limitée par la complexité (au sens de Kolmogorov[2]) du milieu dans lequel elle opère (système d'information). Au-delà, c'est également la décision d'emploi qui est limitée par la difficulté à anticiper totalement les effets et la diffusion de l'arme.

La capacité destructrice est donc souvent cantonnée à ce que plusieurs chercheurs appellent « le sabotage » : c'est-à-dire des actions extrêmement ciblées, équivalent numérique d'un « coup de main » d'une équipe de commandos. Limitées dans leur potentiel destructeur, les armes numériques ne peuvent donc pas être comparées à l'arme nucléaire. La comparaison s'arrête à l'effet dissuasif d'une rhétorique « cyber guerrière ». L'arme numérique entre, en 2013, avec les révélations d'Edward Snowden, dans une nouvelle ère. De fantasmée elle devient une arme d'emploi dont l'usage se généralise et s'ouvre aux acteurs non-étatiques.

Avec la prise de conscience de ces limites et de ces évolutions, l'observation des affrontements dans le cyberespace a rapidement révélé la nature particulière des acteurs en conflit, des cibles engagées, des méthodes utilisées et des buts poursuivis. La « cyber

2. La théorie de la complexité de Kolmogorov permet d'évaluer la complexité de résolution d'un problème sous forme algorithmique. Ainsi, pour une suite numérique S la complexité de Kolmogorov est définie comme la taille, K(S), du plus court programme P qui, confié à une machine universelle, produit la suite S.

guerre » attendue se matérialise avant tout dans le secret des opérations d'espionnage informatique, du vol de données et de la manipulation de l'information. À l'exception de quelques opérations « de grand style » révélées par des compagnies de sécurité informatique, les véritables nuisances ne sont pas du fait de groupes hautement qualifiés déployant des outils d'une technicité sans égale. Les défaçages[3] de sites, les *rançongiciels* ou autres détournements de comptes de réseaux sociaux ne démontrent pas une excellence technique hors du commun. Pourtant, ces opérations simples, parfois rustiques, ont un effet non négligeable sur les cibles visées. Ces effets, qui peuvent être financiers ou organisationnels, portent essentiellement sur l'image de la victime et ne dégradent pas nécessairement en profondeur son système d'information.

Le combat numérique permet donc de conduire une forme de guérilla quotidienne qui ne cherche pas à détruire son adversaire mais dans laquelle les défenseurs s'épuisent à tenter de parer chaque coup. Cette forme de lutte, qui relie des organisations criminelles, des mouvements contestataires et parfois des groupes terroristes, est également utilisée et mise en œuvre par certains États dans le cadre d'une stratégie indirecte.

Les technologies de l'information et de la communication sont donc au cœur d'une révolution dans les mécanismes contestataires. Si elles ne permettent

3. Les défaçages ou défigurations consistent à modifier le contenu d'un site. La modification peut être visible (modification de la page d'accueil) ou plus discrète [Boyer, 2016].

pas totalement d'inverser le rapport de force entre le « faible » et le « fort », elles changent durablement la dialectique du combat et dessinent le contour d'une guérilla 2.0.

Revenons alors à la fable de La Fontaine.

C'est l'invective du lion contre le moucheron, « va-t'en, chétif insecte, excrément de la terre », qui ouvre la fable et enclenche la réaction de l'insecte, « l'autre lui déclara la guerre ». Cet aspect souligne l'importance de ce que l'on appelle aujourd'hui le « champ des perceptions » : le moucheron est humilié par des mots. Il va mettre en œuvre une série de « techniques de guérilla » et renvoie le lion à l'impuissance de sa force. La notion de champ des perceptions revêt dans le contexte actuel un aspect particulier. Les interfaces numériques façonnent les perceptions plus qu'aucun autre système de diffusion de l'information précédent. Les médias traditionnels, que l'on dit en perte de vitesse, ne résistent pas à ces changements. Les opinions se forgent sur les réseaux et se diffusent par leurs intermédiaires. Les *fake news*, ou « infox » s'invitent dans les propos du président des États-Unis et *WikiLeaks* s'érige en censeur des démocraties fragilisées.

« Un avorton de mouche en cent lieux le harcèle : tantôt pique l'échine, et tantôt le museau, tantôt entre au fond du naseau. La rage alors se trouve à son faîte montée. L'invisible ennemi triomphe, et rit de voir qu'il n'est griffe ni dent en la bête irritée qui de la mettre en sang ne fasse son devoir. »

Dans ce combat, la force brute ne parvient pas à obtenir gain de cause. Le moucheron, qui figure ici notre insurgé, décide du début du combat et de sa fin. Comme il engage les hostilités, il en décide du sort. Le lion, épuisé de chasser une mouche insaisissable, n'en peut plus, il laisse à son adversaire la liberté de communiquer sa victoire. Et c'est ici que la chute de la fable nous instruit le plus :

« Comme il sonna la charge, il sonne la victoire, va partout l'annoncer, et rencontre en chemin l'embuscade d'une araignée/Il y rencontre aussi sa fin. »

Le moucheron « franc-tireur », qui vient de sortir victorieux d'un combat que l'on qualifierait aujourd'hui d'asymétrique contre le roi lion, succombe dans les fils de la toile d'araignée. Outre la morale qu'en tire La Fontaine, « qu'aux grands périls tel a pu se soustraire, qui périt pour la moindre affaire », il est intéressant de noter que l'araignée, pour sa part, conduit son combat, elle n'innove pas pour vaincre, ne fait pas preuve d'originalité, son action n'est ainsi pas une « rupture stratégique ». Ainsi si « entre nos ennemis les plus à craindre sont souvent les plus petits », le « stratégiste » La Fontaine nous enseigne également que pour vaincre le moucheron « insurgé », le lion doit s'allier à d'autres dont les modes d'actions, pas nécessairement révolutionnaires, porteront sur les vulnérabilités identifiées de l'adversaire. Ces leçons demeurent valables dans le combat numérique. S'il faut en permanence innover, les organisations les plus structurées en sont parfois incapables. Dès lors,

la victoire réside dans la capacité à tisser des partenariats avec d'autres afin de maximiser son potentiel.

Ce bref voyage dans le temps met en lumière les permanences et continuités du combat asymétrique. Du lion contre le moucheron aux Talibans, des FARC aux *barbudos*, l'insurrection armée traverse l'histoire des conflits et s'adapte aux contingences de l'instant. Les technologies de l'information et de la communication ont-elles modifié la nature de l'affrontement ? La révolte 2.0 est-elle si différente des barricades de 1848 ? Enfin, comment la mondialisation des menaces et les nouvelles formes de terrorisme se nourrissent-elles de la société de l'information ?

La guérilla 2.0 pourrait alors incarner une réponse à ces questions. Véritable insurrection numérique, elle est tout à la fois la transposition de modalités de combats irréguliers dans un espace technique et un type particulier d'acteurs qui trouvent dans le cyberespace les moyens de poursuivre leurs objectifs stratégiques. C'est suivant cette double approche que nous poursuivrons notre étude du concept.

Ainsi, la guérilla 2.0 sera-t-elle, dans un premier temps, étudiée comme une des formes du combat hybride dans le cyberespace. Véritable matrice de l'hybridité, le combat numérique est aujourd'hui pleinement intégré dans les réflexions capacitaires et organisationnelles. L'idée même d'hybridation repose sur la capacité d'un adversaire à manier de façon parallèle des représentations classiques du combat et d'autres plus alternatives ou déviées. Si le concept fait toujours débat, et pour

certains auteurs relève même de la « confusion sémantique », il ne peut toutefois pas totalement être dénigré si l'on en accepte la définition proposée par Élie Tenenbaum : « La guerre hybride pourrait être la combinaison en une seule stratégie, voire en une seule manœuvre des modes de guerre régulier et irrégulier. C'est-à-dire la capacité à combiner ce qu'on appelle la guerre régulière et irrégulière. » [Tenenbaum, 2016].

Qu'elles soient conduites par les armées conventionnelles ou par des intermédiaires (proxys, acteurs privés, milices, partisans…) les opérations hybrides mettent toutes en œuvre des modalités numériques. En ce sens, elles contribuent à l'apparition d'un combattant irrégulier dans le cyberespace. Elles favorisent également l'émergence de nouvelles spécialités liées aux techniques de lutte informatique offensive et la remise aux goûts du jour de concepts qui avaient été parfois négligés ou oubliés à l'image des opérations psychologiques ou de déception.

Pour explorer le concept d'insurrection numérique comme une typologie d'acteur particulier et dépasser la genèse « hybride », il faut dans un deuxième temps étudier les mécanismes révolutionnaires dont la plupart des mouvements insurrectionnels sont issus. L'insurrection est ainsi l'étape ultime d'une de contestation dont l'objectif principal est toujours de renverser un ordre établi pour en substituer un autre. Cette opposition frontale engendre des mécanismes de violences qui n'épargnent aucun acteur et nous amènera à considérer les invariants stratégiques de ce combat. Ce retour

historique et conceptuel sur les insurrections met en lumière le rôle central de l'information dans ce type de combat et pour les groupes y ayant recours.

Dès lors, la bataille ne se joue plus sur un champ clos où s'opposent des forces armées, instruments d'une politique, mais au cœur des populations, sous le regard des caméras. La manœuvre informationnelle et le rapport entre acteurs en conflit et information nous permettra d'ébaucher les principes d'action rendus possible dans le cyberespace.

Que l'on évoque un type nouveau d'acteur irrégulier ou les modalités de l'insurrection, l'étude du phénomène doit s'appuyer sur les différents modes d'action, évaluer leurs impacts, tant, dans ce domaine, c'est l'outil qui fixe le cadre du possible. La guérilla 2.0 se développe ainsi à coups de *hashtags* (mot dièse) sur Twitter, pénètre dans les *smartphones* des plus jeunes avec Periscope, Instagram, Tik Tok ou Snapchat. Les outils de communication portent aujourd'hui bien mal leur nom. Une application Android ou un service d'hébergement en ligne sont bien plus que des outils de communication, ils ne sont pas de simples « tuyaux » passifs qui connectent des « clients » mais bien des outils opérationnels qui peuvent porter et amplifier un combat bien loin de son incarnation physique.

Les outils numériques offrent des services qui dépassent la transmission de données entre deux abonnés et, bien souvent, des débouchés tactiques immédiats. On peut ici évoquer les systèmes de suivi (*tracking*) en temps réel des avions qui permettent d'identifier des

cibles potentielles ou d'analyser une situation tactique (à l'image de la fermeture de l'espace aérien en Crimée en 2013, révélée par les réseaux sociaux) ; Google Earth vous permet de visiter virtuellement des villes, de cartographier des zones entières ; Enfin, la perte progressive de confiance dans les vecteurs classiques d'information (et de façon générale dans les représentations de l'autorité) offre aux diffuseurs en ligne la possibilité de s'exprimer sans aucune garantie sur la nature de l'information qui est relayée.

Cette accélération dans la production de contenus par chaque être connecté, associée à la portée quasi universelle de ces productions, conduit souvent à confondre des notions qui diffèrent pourtant dans leur essence même. Ainsi, ne peut être rangée au rang des modes d'action de l'insurrection numérique la dénonciation publique sur un réseau social ou un blog. Le simple fait d'émettre une opinion, fut-elle en opposition au régime que l'on dénonce, ne constitue pas, à lui seul, un acte de rébellion, même s'il peut être sévèrement réprimandé dans des régimes autoritaires.

Si l'on ne peut donc strictement invoquer le terme d'insurrection (en ligne) pour qualifier la révolte, l'indignation ou l'activisme, une étude de cette réalité nous permettra de mieux en saisir les codes et envisager le point de bascule où, à l'image des révoltes arabes de 2011, cette contestation en ligne mute en insurrection physique pour aboutir à des renversements de gouvernements. Ces évolutions dans les formes de contestation ne sont possibles que dans le contexte de dérégulation des médias

traditionnels. Il nous faudra alors comprendre comment les technologies modifient les métiers de l'information et de la communication pour faciliter l'émergence de ce que l'on qualifie de « guerre de l'information ».

Au service de stratégies étatiques ou d'idéologies mortifères, les techniques et tactiques de guérilla transposées dans les espaces numériques incarnent de nouvelles menaces au potentiel déstabilisateur accru. Les exemples récents qui nous sont offerts par des groupes terroristes djihadistes peuvent servir à comprendre et définir ce combat irrégulier dans le cyberespace. Dans une dernière partie, l'ouvrage propose une réflexion sur les rapports entre terrorisme et espace numérique pour analyser comment un mode d'action extrême de l'insurrection prend corps dans ce nouvel espace, y porte des coups, s'y réfugie mais y est également traqué.

Cherchant à puiser dans la continuité historique tout en y intégrant les modalités actuelles des stratégies hybrides ou des exemples de groupes insurrectionnels ou terroristes, nous chercherons, au terme de notre étude, à comprendre comment une manœuvre peut être pensée et conduite dans l'espace numérique afin de contrer ces menaces. Cette approche large sans être dogmatique pose les bases d'une contre-guérilla 2.0 qui, sans s'affranchir des règles du droit, peut limiter et contraindre l'action des forces irrégulières déstabilisatrices.

Dans ce combat permanent, que l'on peut croire à tort exclusivement technique, la victoire appartient à celui qui saura se renouveler et innover, tant dans ses modes d'action que dans ses organisations.