Décembre 2017

LA LETTRE DU CICDE

Le mot du Directeur

Penser la guerre : telle est l'ambition du CICDE dont les missions s'articulent autour de trois volets interdépendants sur les plans conceptuel et opérationnel : doctrine, retour d'expérience et prospective opérationnelle.

Ces domaines doivent permettre d'imaginer le plus efficacement possible les engagements futurs des armées françaises. Cette vocation du Centre se concrétise en particulier dans sa production doctrinale, qui vise plus largement et concrètement l'efficience opérationnelle de nos armées. Collaborant avec les différentes divisions de l'EMA et de nombreux organismes interarmées, le CICDE anime un réseau qui tend à densifier sa réflexion. Le CICDE ne conçoit en effet sa mission que dans la perspective de l'animation d'un réseau pluridisciplinaire, ouvert sur les grands enjeux sécuritaires, les mutations géostratégiques et technologiques. Sans cela, aussi intelligente soit la réflexion conduite dans nos murs, celle-ci risquerait de rester stérile.

Penser les guerres d'aujourd'hui et de demain dans leur complexité et leur globalité est une absolue nécessité. Mieux cerner les mutations « chromatiques » d'une guerre-caméléon, ses permanences comme ses ruptures, est au cœur des réflexions prospectives qui nourrissent le travail doctrinal du Centre.

Penser la guerre, c'est aussi alimenter la réflexion stratégique au sein du ministère des Armées en refusant ce que certains décrivent comme une « forme d'impuissance de la stratégie ». Démarche indispensable, sauf à prendre le risque de se laisser surprendre au-delà de l'acceptable, l'anticipation participe en outre d'une obligation de créativité stratégique.

Dans cette perspective, le Centre vous propose une lettre du CICDE, rénovée dans sa forme, sur un sujet d'actualité : la désinformation.

Le champ des perceptions est en effet un champ de bataille à part entière, sur lequel se déchaînent de façon discrète et parfois occulte des adversaires mal intentionnés. Plus que jamais la résilience d'une organisation ou même d'une nation, face à ces attaques ou à ces menaces, impose une prise de conscience des enjeux réels mais aussi de nos vulnérabilités. C'est à cela que vous invitent les différents articles de cette lettre.

Général de division Antoine Windeck

Sommaire :

Vous avez dit « désinformation » ?

« *On ne ment jamais tant qu'avant les élections, pendant la guerre et après la chasse.* »

Georges Clémenceau

Une pratique ancienne et actuelle

« *Depuis que les hommes ont une bouche pour parler, des oreilles pour entendre, autrement dit depuis qu'ils échangent des messages, ils ont compris qu'il est possible de tirer avantage du flou propre à la plus innocente des informations ; que, l'aloi de vérité qui y est compris n'étant ni fixe, ni garanti, il n'y a rien de plus facile que de joindre à l'approximation involontaire la tromperie délibérée.* » Ainsi s'exprimait Vladimir Volkoff dans « *La Désinformation, arme de guerre* », ouvrage paru en 1996.

Désormais, il ne se passe pas une journée sans que soient évoqués souvent pour les dénoncer, parfois pour les propager des rumeurs ou fausses nouvelles (*fake news*) ou des canulars (*hoax*) qui semblent être devenus les principales sources d'animation des media et des réseaux sociaux. Une nouvelle notion est même née : la post-vérité (*post-truth*). Élu « mot de l'année 2016 » par l'*Oxford English Dictionary,* cette expression désigne des circonstances dans lesquelles les faits objectifs ont moins d'influence pour modeler l'opinion publique que les appels à l'émotion et aux opinions personnelles. De nouveaux métiers comme celui de vérifieurs de faits (*fact-checkers*) voient également le jour : traquant les rumeurs, les fausses nouvelles et les canulars, ces gardiens de la vérité malmenée par les approximations, les exagérations ou autres amalgames sont censés la « rétablir » en rapprochant ce qui est dit des faits réels.

On peut toutefois s'interroger sur la sincérité de cette vigilance inédite : alors que la désinformation est aussi vieille que l'humanité et que les media traditionnels en étaient auparavant les colporteurs tout autant que les media numériques aujourd'hui, ils n'ont jamais suscité pour autant une réaction de cette ampleur. N'assisterions-nous pas au développement d'une vaste campagne de désinformation dans ce cadre ?

Le sujet est donc plus que jamais d'actualité, comme en atteste le titre de la dernière livrée 2018 du Rapport Annuel Mondial sur le Système Économique et les Stratégies (RAMSES 2018) édité par l'Institut Français des Relations Internationales (IFRI) : la guerre de l'information aura-t-elle lieu ?

Dans ce contexte et dans cette guerre, nos armées sont-elles impliquées ? Le cas échéant, que peuvent-elles faire aujourd'hui et demain face à la désinformation ?

Manipulation en tous genres

Mais avant toute chose, il convient de définir ce qu'est la désinformation. En guise de point de départ, laissons s'exprimer une nouvelle fois Vladimir Volkoff, cette fois-ci dans « *Petite histoire de la désinformation* » qui tente de la cerner en expliquant ce qu'elle est et ce qu'elle n'est pas : « Il semble que la désinformation suppose trois éléments :

- une manipulation de l'opinion publique, sinon ce serait de l'intoxication ;
- des moyens détournés, sinon ce serait de la propagande ;
- des fins politiques internes ou externes, sinon ce serait de la publicité. »

Pour lui, « la désinformation est une manipulation de l'opinion publique à des fins politiques avec une information traitée par des moyens détournés. » Plus que de la production de faux, la désinformation procède d'une falsification mettant en perspective un certain nombre d'éléments parcellaires pas forcément liés mais conduisant inévitablement à un raisonnement et à des déductions erronés.

On comprend alors que combattre la désinformation n'est pas chose aisée et qu'à défaut de l'éradiquer totalement, ce qui semble être un objectif inaccessible, il vaut peut-être mieux s'attacher à en limiter les effets néfastes. Pour y parvenir, il ne suffit pas uniquement de chercher à neutraliser les sources émettrices de désinformation ou de préserver la justesse des informations par rapport à la réalité qu'elles recouvrent ; il faut également pouvoir vérifier la traçabilité de l'information en agissant sur les canaux de transmission qu'elle emprunte.

Les armées ont déjà pris en compte la désinformation. Elles la définissent par son mode d'action : « [Elle] … *manipule l'information par le mensonge et/ou le travestissement de la réalité dans le but de donner une compréhension erronée des situations*[1]. »

« La désinformation manipule l'information par le mensonge et/ou le travestissement de la réalité dans le but de donner une compréhension erronée des situations. »

Ne pas la favoriser, s'en prémunir, la combattre

Pour tenter d'en atténuer les effets, il faut tout d'abord commencer par ne pas la favoriser. À cet effet, une mesure de défense passive pour les armées consiste à ne communiquer que des faits avérés, vérifiés et vérifiables par les destinataires de l'information. Il vaut donc mieux délivrer une information exacte même incomplète « *car informer au plus tôt, afin de donner le ton à la communication, évite la propagation de rumeurs ou d'interprétations erronées, voire les tentatives de désinformation*[2] ». Plus que jamais, dans le contexte actuel, la transparence est supposée être un gage de vérité.

Par ailleurs, et c'est une constante dans les armées, l'application d'un processus et du principe de multiplicité constitue une mesure active pour se prémunir de la désinformation : « *le principe de multiplicité est de faire appel à plus d'une source pour recueillir la même information. Il donne une plus grande assurance de succès dans le recueil de l'information, favorise le recoupement de l'information recueillie, consolide le renseignement élaboré et représente une protection contre les actions de déception adverses*[3]. »

Désinformer pour combattre la désinformation se révélerait plus contre-productif que contre-offensif, tant il est vrai qu'une somme de désinformations contradictoires n'est jamais nulle ; non seulement la désinformation majoritairement mais pas exclusivement adverse ne serait pas forcément neutralisée mais, de surcroît, il en résulterait un brouillage définitif de tout repère en lien avec la réalité créant ainsi une confusion rendant impossible la compréhension de cette réalité. Si désinformer peut servir à influencer, en revanche influencer n'est pas désinformer : c'est même le moyen le plus efficace dont disposent les armées pour lutter contre la désinformation comme en atteste l'article suivant.

Un enjeu croissant

Enfin, à l'avenir, l'enjeu représenté par la capacité à lutter contre la désinformation devrait encore augmenter : « *En 2035, le point de concentration des émotions et des perceptions sera devenu déterminant car c'est là que se croiseront et fusionneront potentiellement émotions, informations, contre-informations, manipulations individuelles et désinformation collective. En 2035, ce point nodal immatériel pourrait, dans certains cas, représenter à lui seul l'enjeu d'une manœuvre globale au service d'une stratégie d'ensemble de long terme et faire basculer l'issue d'un affrontement.*

Toute stratégie victorieuse nécessitera un contrôle des champs immatériels (cyberespace et informationnel), afin, notamment, de remporter la bataille des perceptions dans un contexte global[4]. »

À ce propos, on peut se demander si les armées ne devraient pas s'orienter vers une intégration de la technologie ou de la logique de type *blockchain* qui, en sécurisant davantage le stockage et la transmission d'informations, augmenterait ainsi leur résilience face à la désinformation tout en restant compatible avec ce qui pourrait devenir la norme en matière de diffusion de l'information. Quoi qu'il en soit, les armées doivent redoubler de vigilance, analyser méthodiquement les nouvelles menaces provenant d'acteurs variés exploitant les rapides évolutions des technologies de l'information et de la communication et s'y adapter. Sinon, la guerre de l'information pourrait avoir lieu sans elles.

COL. (T) Jean-François Lagrange
Sous-direction « doctrine »

Notes de l'auteur :

(1) Doctrine interarmées (DIA)-3.10.1(A), *Opérations psychologiques*, n° 182/DEF/CICDE/DR du 16 septembre 2016.

(2) Doctrine interarmées (DIA)-3.40, *Communication Opérationnelle*, n° 297/DEF/CICDE/NP du 26 juillet 2007 (ex DIA-3.10.2).

(3) Publication interarmées (PIA)-2(A), *Procédures du Renseignement d'Intérêt Militaire*, n° 18715/DEF/DRM/DR du 7 décembre 2011.

(4) Réflexion prospective interarmées (RPIA)-2016/001, Environnement opérationnel futur 2035, n° 101 /DEF/CICDE/DR du 23 mai 2016, version amendée le 11 juillet 2017.

Bibliographie :

- HARBULOT Christian, *La guerre cognitive, l'arme de la connaissance*, Éditions Lavauzelle, Paris, 2004.
- HARBULOT Christian, *Fabricants d'intox, la guerre mondialisée des propagandes,* Éditions Lemieux, Paris, 2016.
- KLEN Michel, *Les ravages de la désinformation d'hier à aujourd'hui*, Éditions Favre, Lausanne, 2013, *ISBN* 978-2-8289-1335-9.
- LEFORT-LAVAUZELLE Patrice, *Comprendre la technologie du* blockchain*. Quelles applications dans la défense ?*, Revue Défense n° 187, juillet-août 2017.
- VOLKOFF Vladimir, *La désinformation, arme de guerre*, Éditions Julliard/L'Âge d'Homme, Paris, 1986, Lausanne, 2004, 274 p., *ISBN* 2-8251-0333-0.
- VOLKOFF Vladimir, *Petite histoire de la désinformation*, Éditions du Rocher, Paris, 1999, 289 p., *ISBN* 2-268-032-019.

Quelle place pour les armées dans la lutte contre la désinformation ?

Les armées doivent donc intégrer la désinformation dans le champ de leur action, que ce soit en amont des opérations, dans le cadre de l'appréciation autonome de situation, comme en opération, dans la planification et la conduite de l'action.

La désinformation s'adresse aux masses et touche toutes les sphères de l'activité humaine

La désinformation manipule l'information par le mensonge ou le travestissement de la réalité, dans le but de donner une compréhension erronée des situations et d'amener l'auditoire lui-même à des conclusions parfois sans lien direct avec les faits réels mobilisés pour élaborer la désinformation. Elle s'adresse d'abord aux masses, qu'elle cherche à faire douter, à déstabiliser, ou inversement à renforcer dans une compréhension erronée des choses. Au contraire de la propagande, elle n'a pas d'apparence contraignante et ne dicte pas explicitement des idées ni des comportements, mais y amène le plus souvent de façon indirecte, en présentant les éléments d'information de sorte que, progressivement, l'auditoire fasse de lui-même les liens entre eux vers la conclusion souhaitée. À la différence de la propagande encore, elle ne permet pas de distinguer facilement le but ni le commanditaire.

À une époque où domine en Occident un relativisme philosophique qui tend à séparer de plus en plus le raisonnement et le débat de l'observation factuelle du réel, la désinformation est une pratique qui touche toutes les sphères de l'activité humaine, pour faire valoir des intérêts, promouvoir une représentation du monde, ou encore dissimuler des intentions.

Le plus souvent, la désinformation modèle l'environnement informationnel[1] (EI), c'est-à-dire qu'elle crée dans les opinions publiques les conditions qui favorisent la prise de décision par les autorités en place, dans le sens souhaité par l'émetteur de la désinformation. Ainsi, au plan géopolitique, les exemples ne manquent pas, à notre époque, de l'usage de la désinformation pour préparer ou justifier l'emploi de la force, bien souvent pour contourner les principes du droit international.

La désinformation sur Internet et les réseaux sociaux, qui fait la Une de l'actualité médiatique et politique, n'est donc pas un phénomène fondamentalement nouveau, mais les caractéristiques propres à ces vecteurs permettent d'en décupler potentiellement l'efficacité. Sans chercher l'exhaustivité, mentionnons la vitesse, la portée, le rôle simultané de créateur-émetteur-récepteur d'information de tout utilisateur (sous son identité ou sous avatar), le rôle de « caporal stratégique » joué par le moindre individu sachant exploiter les possibilités du système. Soulignons également la difficulté d'attribuer la paternité d'une action ou d'un message à l'acteur qui souhaite rester anonyme, difficulté dont le corollaire est la possibilité de faire attribuer à Paul ce qui vient de Jean, ce qui constitue en soi un élément majeur de désinformation.

Préoccupation légitime pour les armées

Dans la mesure où une partie des actions de désinformation peut constituer une menace pour la souveraineté et la sécurité nationales, l'État est évidemment légitime à intervenir au titre de ses attributions régaliennes. La lutte contre la désinformation consiste alors, simultanément, consécutivement ou alternativement, à s'attaquer à l'émetteur, à rétablir l'information véridique, à « décontaminer » l'auditoire touché par la désinformation, et à juguler les effets négatifs générés par celle-ci. Si l'État ne peut prétendre au monopole de la lutte en la matière, il peut en prendre l'initiative, conseiller, appuyer voire coordonner les acteurs de la société civile.

Les armées sont concernées à double titre :

- d'une part, dès lors que la France envisage d'utiliser ses forces armées dans la gestion d'une crise, celles-ci peuvent être confrontées à des actions de désinformation, qui peuvent les cibler directement, dans le cadre de procédés d'intoxication[2] par exemple ;
- d'autre part, leurs membres sont des citoyens ayant accès aux mêmes sources d'information/désinformation que leurs compatriotes, comme eux, ils peuvent en être les victimes, voire les relais involontaires lorsqu'ils contribuent à la diffusion de cette désinformation.

Les armées doivent donc intégrer la désinformation dans le champ de leur action, que ce soit en amont des opérations, dans le cadre de l'appréciation autonome de situation, comme en opération, dans la planification et la conduite de l'action. Pour ce qui ne ressortit pas à leur champ d'action, elles peuvent apporter aux autres outils régaliens un appui méthodologique.

Des principes d'action

Dans tous les cas, il s'agit des principes et mécanismes décrits au sujet de la stratégie militaire d'influence et du processus *Info Ops*[3]. Ils sont facilement transposables en dehors de la sphère militaire et reposent sur un cycle articulé de la façon suivante :

1. **Veiller, analyser, comprendre** ce qui se passe dans l'environnement informationnel. Il s'agit notamment de détecter les signaux faibles trahissant l'émission/dissimulation **intentionnelle** d'informations, qu'elles soient avérées, ou partiellement ou totalement construites.

   L'objectif est de pouvoir établir de la façon la plus précoce possible des hypothèses concernant **les intentions et actions** d'acteurs potentiellement hostiles : quels effets, sur quels auditoires nationaux ou amis, avec quels vecteurs, combinant quels messages et quelles informations réelles ou non, et enfin avec quels effets avérés, ces acteurs cherchent-ils à obtenir ?

2. **Planifier**. En fonction de cette matrice, des conséquences potentielles sur l'opinion publique, les décideurs, et les outils régaliens nationaux, il s'agit de définir quels effets l'on veut obtenir en retour, effets qui se répartissent essentiellement entre :

   - les auditoires des actions de désinformation hostiles, qu'ils aient déjà été touchés (effets de décontamination), qu'ils ne l'aient pas été (effets de protection) ;
   - les émetteurs des actions de désinformation, **ainsi que leurs relais intentionnels ou non** (effets de neutralisation, de dissuasion pour la suite) ;
   - l'information erronée elle-même (effets de révélation, d'oblitération…) ;
   - l'ensemble pouvant s'inscrire dans une manœuvre informationnelle globale.

3. **Conduire**. Il s'agit de coordonner dans les espaces (monde « réel » et cyberespace en particulier) et dans le temps (immédiateté et terme plus long) les actions de tous ordres (informationnelles, physiques) qui permettent d'obtenir les effets de contre-désinformation planifiés.

4. **Évaluer**. À partir de critères prédéterminés, il s'agit d'apprécier l'effet de la manœuvre informationnelle de neutralisation de la désinformation dans les trois volets évoqués au paragraphe 3.

Les moyens d'une stratégie

Désinformation et contre-désinformation sont donc bien des modalités d'une stratégie d'influence, dans son volet défensif puis contre-offensif.

Le défi majeur demeure celui de l'analyse et de la détermination de ce qui est désinformation. Outre la difficulté technique, accrue par la multitude de logiciels permettant de « retoucher » le matériau originel, et de se dissimuler dans le cyberespace, le défi à relever est celui de la cotation, et de l'objectivité de celui qui en a la charge. Il faut pour cela des analystes certes experts techniques de leur domaine, mais aussi d'une grande probité morale, capables d'analyser les choses avec l'objectivité de l'entomologiste penché sur son vivarium, **et conscients de leurs propres biais cognitifs**.

À défaut de cela, il existe un risque de voir la lutte contre une forme de désinformation devenir l'instrument d'une nouvelle désinformation, dans le cadre de débats idéologiques où ce mot devient un anathème jeté à la figure de l'adversaire, notamment pour le discréditer aux yeux de l'opinion[4].

Ceci implique de développer des outils permanents de veille et d'analyse de l'EI, et singulièrement du cyberespace et de la myriade constamment évolutive des réseaux sociaux, et de se doter de la ressource humaine, nombreuse et qualifiée, pour assurer cette mission de souveraineté.

Pour l'heure, alors que l'OTAN entame un effort conséquent en la matière, et que la capacité et la créativité des plus grandes puissances ne sont plus à démontrer, **la France n'est pas encore totalement entrée dans cette approche résiliente**.

COL. (T) Hervé Kirsch
Sous-direction « Doctrine »

Notes de l'auteur :

(1) L'environnement informationnel *« comprend l'information elle-même, les individus, organisations et systèmes qui la reçoivent, la traitent et la transmettent, et l'espace cognitif, virtuel et physique dans lequel cela se produit »* (DIA-3.10).

(2) Voir DIA-3.10.1(A), *Opérations psychologiques*, septembre 2016.

(3) Voir DIA-3.10(A), *Stratégie militaire d'influence et opérations d'information*, juin 2014, version amendée en mars 2016.

(4) Voir la polémique suscitée par la création du « DECODEX » : https://blogs.mediapart.fr/denis-dupre/blog/240817/l-inquisition-decodex-qui-vient-ruffin-l-index

Aspects prospectifs concernant la lutte contre la désinformation

Des progrès dans sa détection

L'augmentation de la puissance des moyens de diffusion des idées et d'action sur les opinions : imprimerie, transports, cinéma-radio-télévision et désormais Internet et les réseaux sociaux, permet de toucher presque n'importe qui, en s'affranchissant des problèmes de distance, de temps et même, à l'heure actuelle, de langages.
Ces moyens pouvant être utilisés de manière malhonnête, à des fins de déstabilisation, il est nécessaire de disposer de la capacité de s'en protéger.

De nombreux travaux sont en cours afin de concevoir ou d'améliorer des outils et des structures permettant de détecter les actions de désinformation et, dans la mesure du possible, d'en neutraliser les sources ou leurs effets.
Le développement d'outils informatiques, facilement accessibles, permettant de modifier, donc de falsifier, des documents, images, fichiers sonores ou vidéo, associé aux possibilités offertes à tous de diffuser des informations sur Internet, constituent actuellement les principaux moyens de désinformation.

Les progrès importants réalisés, dans le domaine du traitement de l'information et de l'analyse en masse des données, permettent de détecter certaines de ces manipulations. Des études sont en cours pour améliorer les outils d'aide à la mise en évidence de modifications d'un fichier informatique, en particulier pour les images ou les métadonnées : date, origine, titre, etc.

Un autre axe consiste à développer les moyens permettant de faire ressortir les incohérences au sein d'une masse de données. Ces moyens doivent nécessairement comporter des experts humains, des méthodes et des outils informatiques.

Un support informatique falsifié pourra, par exemple, être identifié par comparaison avec ses supports source, par le suivi de ses évolutions, si possible en détectant les acteurs : sur quels ordinateurs, par quels réseaux, à quel moment, etc.

Ces moyens peuvent également permettre de détecter et de suivre l'apparition et la diffusion de rumeurs, de fausses informations ou de données sorties de leurs contextes.

Le développement d'outils informatiques, facilement accessibles, permet de modifier, donc de falsifier, des documents, images, fichiers sonores ou vidéo.

L'effort pour disposer de la capacité de détection de ces incohérences (et autres « signaux faibles ») ne peut se relâcher car la quantité de données augmente très rapidement et l'efficacité dépend aussi des délais de réaction. De plus, les moyens utilisés pour la désinformation progressent aussi.

Disposer d'outils adaptés au besoin

Pour assurer une efficacité maximale, des efforts doivent être poursuivis afin de permettre, en plus de pouvoir capter et traiter en temps contraint des quantités énormes de données, d'améliorer les interfaces restituant l'information aux experts humains et, surtout, permettant à ces experts humains de travailler de manière interactive dans un cadre multidisciplinaire.

Les travaux en cours sur les outils informatiques permettent de toujours mieux transcrire et traduire des textes, écrits ou parlés, reconnaître et extraire des éléments d'intérêt dans les images ou les fichiers sonores.

Le développement des capacités de calcul permet d'analyser simultanément un grand nombre de paramètres et de toujours mieux identifier des objets, des personnes, des attitudes, des voix, etc. à travers d'énormes corpus de données, le rôle de l'expert humain étant de paramétrer ces outils (en général en fournissant des exemples de ce qui doit être reconnu à partir de grands ensembles de « données modèles ») d'orienter ou de superviser puis de valider et d'interpréter les résultats.

Des progrès sont également enregistrés avec les outils d'analyse sémantique qui permettent de reconnaître, d'extraire et de comparer, non seulement des parties de phrases et des entités, mais aussi, toujours plus facilement, les éventuels aspects positifs ou négatifs, ironiques, etc., ainsi que des éléments qui permettent d'identifier des idées ou des arguments.

Ces outils permettent également d'identifier le style ou autres caractères distinctifs de l'auteur.

S'il est possible de modifier quelques paramètres de certaines données, il devient difficile de falsifier une information complexe sans que cela puisse être détecté car le recoupement des multiples grandeurs caractérisant cette information mettra probablement en évidence des incohérences.

Le boulet et la cuirasse

Cela pourrait conduire à une course technologique entre les moyens de falsification et les moyens de détection de ces falsifications. Par exemple, pour réaliser une séquence vidéo qui attribuerait un discours ou un comportement choquant à un acteur que l'on veut discréditer, en restituant sa voix, ses gestes ou ses expressions.

L'utilisation de moyens automatiques d'analyse sémantique devrait faciliter le suivi de la propagation des idées et des arguments, identifier les réactions qu'ils provoquent et comment les différents acteurs les interprètent, les reprennent, les acceptent ou les combattent. Ces moyens permettraient donc de faciliter la détection et la compréhension des actions de désinformation mais aussi d'anticiper sur leurs conséquences, ainsi que de reconnaître les auteurs et leurs intentions. Ils permettent aussi d'aider à construire des supports de communication optimisés pour la « contre-désinformation ».

La connaissance des paramètres caractérisant le contexte, les particularités des différents acteurs permet aussi de modéliser et de simuler de manière toujours plus fine des scénarios intégrant des actions de désinformation. Ces moyens permettent d'étudier comment et pourquoi les différents types d'acteurs (populations, dirigeants, forces, amis, potentiellement hostiles, etc.) sont susceptibles d'être touchés ou concernés, lorsque c'est en rapport avec des crises menaçant notre sécurité, et de modéliser quels types d'actions de désinformation pourraient les atteindre afin de mettre en place des actions de protection ou de prévention.

D'une manière générale, permettre d'identifier nos points forts et nos éventuelles faiblesses face aux différents types d'actions de désinformation.

Une nécessaire approche globale

Les progrès rapides et continus des outils informatiques ne doivent pas nous faire oublier qu'Internet n'est pas le seul support possible pour mener des actions de désinformation et que les rumeurs transmises de bouche à oreille, la circulation de documents papier, restent des moyens efficaces, en particulier au sein de communautés déplacées ou dans le cadre de mouvements importants de population.

Si les actions de désinformation peuvent avoir des conséquences sur la liberté de conduire les opérations militaires, elles sont susceptibles d'être dirigées contre tous les facteurs de puissance, en particulier l'économie et la culture, il est donc indispensable de les aborder dans le cadre d'une « approche globale ». Cela est d'autant plus important que les acteurs de certains de ces milieux, comme la bourse ou les médias, sont particulièrement sensibles aux rumeurs et ont un effet démultiplicateur auprès des populations que nous avons le devoir de protéger.

Des structures se mettent en place, dans un cadre national ou international, pour lutter contre la désinformation, en intégrant en particulier des journalistes, le domaine d'action de ces structures aura nécessairement des limites : même en étant de bonne foi, des faits peuvent être interprétés différemment en fonction de la culture, de l'histoire collective ou personnelle, etc. et donc conduire à des « vérités » différentes.

Comme le cas de la lutte informatique, il est parfois difficile d'identifier le ou les véritables acteurs à l'origine de la désinformation, leur objectif pouvant être de créer des tensions entre deux pays, entités ou communautés aux moyens d'actions que l'une des parties attribuera à l'autre.

Il est donc indispensable de pouvoir disposer d'une capacité de détection et de réaction autonome, ou du moins maîtrisée ou contrôlable, ne serait-ce que parce que des actions à la limite de la désinformation, conduites par des entreprises privées, des organisations criminelles, des ONG, etc. peuvent agir indirectement sur nos capacités en portant atteinte à nos structures sociales ou économiques et ne seront pas reconnues comme étant de la désinformation par tous nos partenaires ou alliés.

ICETA Éric Pfannstiel
Sous-direction « Prospective opérationnelle »

Focus RETEX – Principaux enseignements tirés de la bataille de Mossoul

Initiée le 17 octobre 2016, l'opération de reprise de la ville de Mossoul (opération *STRIKE EAGLE*) s'est achevée le 10 juillet 2017, après neuf mois de combats acharnés. Ces combats en zone urbaine ont été d'une ampleur inégalée depuis la bataille de Stalingrad (1942-1943), et diffèrent d'autres grandes villes d'Irak, comme Falloujah ou Ramadi, dont la population avait été en grande partie évacuée.

Cette bataille a une nouvelle fois confirmé que le milieu urbain est un terrain particulièrement complexe, vivant et peuplé, très changeant et favorisant amplement les systèmes défensifs. Les combats s'y déroulent à la fois en surface, dans l'espace aérien (3D), ou encore en sous-terrain. Daesh a ainsi utilisé à son avantage les caractéristiques du milieu urbain (emploi de tunnel, d'abris souterrains, de *bunkers*, dissimulation dans les bâtiments ou au sein de la population, camouflage par dispersion de fumée [pneus, dépôts de souffre, etc.] ou encore utilisation de leurres). Connaissant les règles d'engagement de la coalition, il n'a pas hésité à s'abriter dans des écoles, hôpitaux, mosquées, et à utiliser les populations civiles comme bouclier humain. Daesh a en outre fait preuve d'une très grande capacité d'adaptation en employant des technologies duales et des produits de grande diffusion qu'il a su rapidement militariser. L'emploi généralisé de *VBIED (Vehicle Borne Improvised Explosive Devices)*, d'armes chimiques rudimentaires, ou encore de mini drones (*ISR*, guidage, largage d'obus) a ainsi démontré une grande capacité d'innovation.

L'analyse de cette bataille fait ressortir les principaux enseignements suivants :

Une zone de combat complexe et abrasive

Dans l'environnement complexe et très changeant qu'est une zone urbaine, un renseignement robuste et réactualisé en permanence est un prérequis indispensable.

La rusticité et l'abrasivité du terrain ont terriblement affecté les matériels (les pneus de véhicules ont par exemple beaucoup souffert), mais également les combattants opérant dans un environnement marqué par la présence de microparticules contre lesquelles ils ne disposaient pas d'équipement de protection adéquat. Le terrain permettait difficilement l'atterrissage d'hélicoptères à proximité, raison pour laquelle de nombreuses équipes médicales ont été intégrées aux groupes de combattants.

L'emploi généralisé et à grande échelle de munitions de précisions (guidées GPS), à faibles dommages collatéraux ou encore d'armements à tir direct (type *Hellfire* ou *Brimstone*), ainsi que la bonne adaptation des effets de ces munitions au milieu urbain (bâtiment de plusieurs étages, béton particulier, angles d'attaque, caractéristiques urbaines atténuant ou amplifiant les effets) posent la question de l'adéquation de nos propres munitions à l'environnement urbain.

Afin d'optimiser le tir de munitions de précision guidées GPS, l'extraction et la certification de coordonnées précises sont devenues des prérequis indispensables. La gestion des stocks de munitions qui a affecté de nombreux pays, dans un contexte de tirs intensifs, a également été une problématique soulevée au cours de cette bataille.

La gestion des personnes déplacées est un paramètre essentiel, compte tenu de l'incidence sur les opérations. Ce paramètre est à prendre en compte dans les opérations militaires tant en conduite qu'en planification. La coopération avec les ONG est, à ce titre, impérative avec une sensibilisation préalable souhaitable.

Des fonctions opérationnelles essentielles

Les opérations ont été particulièrement centrées sur « l'image », mais l'emploi de moyens et de bases de données très différents a perturbé la cohérence d'ensemble. La standardisation et l'interopérabilité de ces moyens pour obtenir une *COP* (*Common Operational Picture*) unique et cohérente, notamment pour le ciblage, sont devenues un enjeu majeur. Si les moyens ISR ont été cruciaux, ils n'ont cependant pas été suffisants et le renseignement d'origine humaine (ROHUM) ne doit pas être relégué au second plan.

La mobilité des forces attaquantes (FSI) a été très rapidement réduite sur un terrain rendu très chaotique et canalisant par Daesh (*IED*, *snipers*). L'emploi de blindés lourds et peu manœuvrants a été rendu difficile, tandis que l'emploi de véhicules légers s'est avéré plus adapté à un tel environnement dégradé. Pour faire face au défi de la mobilité, le *bulldozer* blindé est devenu un élément essentiel pour briser les différents barrages à un point tel qu'il est devenu par la suite l'une des cibles privilégiées de Daesh. L'appui à la mobilité a ainsi été primordial pour permettre l'avancée des troupes en zone urbaine.

En matière de frappes aériennes, le processus de ciblage en temps réel a été bien plus utilisé que celui du ciblage planifié. La quantité conséquente de cibles a nécessité l'emploi de *JTAC* en grand nombre. Comme pour les avions, dont l'appui a été fondamental et pour lesquels la maîtrise de la 3ème dimension a été un prérequis indispensable, les hélicoptères ont également été bien plus employés en *CAS* (*Close Air Support*) qu'en *CCA* (*Close Combat Attack*) et ont offert un appui tout aussi intéressant, avec des angles d'attaque (horizontaux) complémentaires de l'armement délivré par les avions (vertical). Dans ce cadre enfin, le *Battle Tracking* des amis (*Blue Force Tracking*) s'est avéré indispensable pour éviter, ou à défaut limiter, les tirs fratricides.

Les *Strike Cells* ont joué un rôle clef en tant qu'éléments intégrateurs et centralisateurs des appuis feux interarmées, notamment du fait de moyens SIC extrêmement performants rendant possible la centralisation des autorisations d'engagement. Néanmoins en cas de rythme intensif des opérations imposant des délais réduits de validation des tirs, il a été observé une décentralisation des appuis feux, à travers la délégation de certaines autorisations d'engagement (principalement pour des tirs aériens) vers les niveaux tactiques.

Mossoul a été un cas d'école très intéressant en matière de PMO (partenariat militaire opérationnel avec les forces locales irakiennes). Les Américains ont d'ailleurs créé une brigade spécialisée dédiée à cette fonction.

Des capacités nouvelles à prendre en compte

Le retour de la guerre électronique (GE) et du NRBC : l'environnement électromagnétique (EM) s'est avéré être un champ de bataille contesté par l'ennemi et a nécessité une gestion à part entière par les états-majors de la coalition. Le spectre EM est bien un espace de bataille à part entière, dans lequel des « effets militaires » sont obtenus, lui donnant une importance centrale dans les combats futurs. Dans un autre registre, l'emploi régulier d'armement NRBC, certes rudimentaires, par Daesh, impose une réflexion capacitaire complète de lutte contre cette menace, incluant équipements et entraînement.

Mossoul a démontré le bénéfice tactique qui pouvait être tiré de l'emploi de mini-drones du commerce sur le champ de bataille, notamment en zone urbaine. Daesh en a fait un emploi quasi industriel et les FSI ont également largement utilisé des quadricoptères (notamment le DJI *Phantom*) très manœuvrables (plus que les voilures fixes manquant d'espace ouvert) et faciles d'emploi. Déjà identifié en RCA, ce constat pose la question de l'acquisition de tels moyens pour nos propres forces. *A contrario*, l'obtention d'une capacité interarmées de lutte anti-drone est devenue aujourd'hui un véritable enjeu de sécurité des combattants.

Le soutien en « génération électrique » du combattant a

Cette bataille a confirmé que le milieu urbain est un terrain particulièrement complexe, favorisant amplement les systèmes défensifs.

enfin été une problématique soulevée au cours de cette bataille, compte tenu d'équipements de plus en plus nombreux dépendant de cette ressource.

L'adaptation : une capacité essentielle des combattants et des organisations

Adversaire asymétrique, Daesh a su rapidement s'adapter en exploitant l'environnement et en tirant parti au maximum de ses ressources, pour inverser en sa faveur un rapport de force très défavorable (5000 contre 90 000 soit un RAPFOR de 18 contre 1) et faire face à un adversaire technologiquement supérieur. Les forces irakiennes et la coalition ont également dû faire preuve d'adaptation et d'innovation rapides pour éviter des pertes trop nombreuses, à travers par exemple le principe du « *cratering* »[1] pour limiter la liberté d'action des *VBIED* ennemis.

Le rythme d'adaptation de l'ennemi dans un environnement technologique très évolutif impose de raccourcir notre propre boucle d'acquisition et d'emploi de nouvelles capacités, en particulier l'acquisition de nouveaux équipements (au besoin sur étagère), au risque de se faire dépasser, en particulier en matière d'emploi de drone, de LAD (lutte anti-drone), de GE, de NRBC et de *C-IED* et ainsi de perdre la supériorité opérationnelle.

Comme auparavant, cette bataille a une nouvelle fois illustré la nécessité de faire tourner notre propre boucle OODA[2] plus rapidement que celle de l'adversaire pour pouvoir créer des opportunités. La capacité d'adaptation sera aujourd'hui, encore plus qu'hier, une qualité maîtresse du combattant. Il devra être en mesure de savoir mettre en œuvre des technologies qu'il n'aura pas eu le loisir de maîtriser auparavant.

COL. (A) Éric Le Mouël
Sous-directeur « RETEX »

Notes de l'auteur :

(1) Réalisation de « cratères » dans les rues ou les routes, par tirs de munitions (bombes, obus, etc.).
(2) Observation, Orientation, Décision, Action.

Drone armé artisanal utilisé par Daesh

Les dernières parutions…

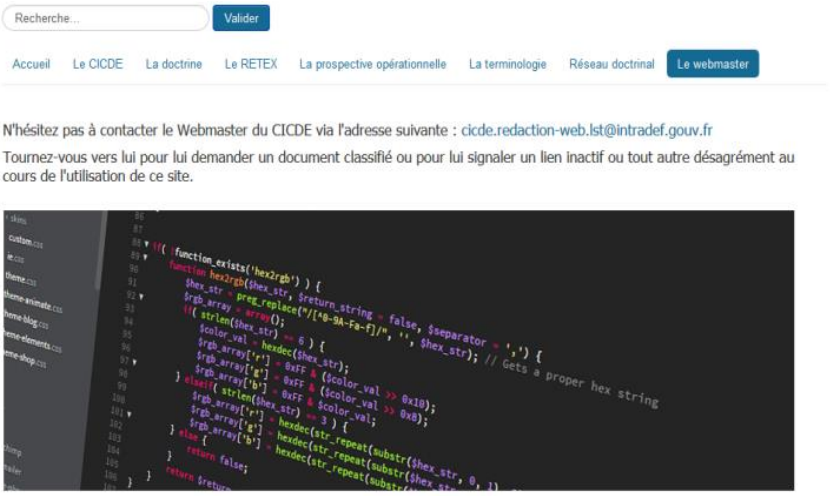
	**DIA-3.2.5(A)_GPC(2017)** « Gestion des personnes capturées » du 5 octobre 2017 (**DR**) Résultat d'un travail collaboratif, le présent document actualise la version 2011 de la doctrine interarmées (DIA) traitant de la gestion des personnes capturées. S'appuyant sur le retour d'expérience des dernières opérations extérieures menées par la France, cette doctrine révisée traite de la gestion des prisonniers de guerre et des personnes retenues, que ce soit dans le cadre d'un conflit armé international ou non international. À cette fin, sont ainsi détaillées les règles relatives à la gestion des personnes privées de liberté, de leur capture à leur libération ou à leur traduction devant un tribunal compétent.
	**DIA-3.6(A)_GUERELEC(2017)** « La guerre électronique – Supplément français à l'*AJP-3.6* » du 20 octobre 2017 (**DR**) L'armée de Terre des États-Unis a récemment conduit un retour d'expérience (RETEX) sur la bataille de Mossoul, et l'un des points qui en ressort est la difficulté d'opérer dans un environnement électromagnétique à la fois saturé (tous les acteurs ont besoin des fréquences pour leurs communications) et très contesté (certains acteurs possèdent une guerre électronique très élaborée). C'est dans ce contexte de réflexion que paraît la DIA-3.6(A) *Guerre électronique (GE)*. Ce document remplace une ancienne version qui n'était pas d'ordre doctrinal. Celle-ci est la première véritable doctrine interarmées de GE. Elle se fonde sur la doctrine de l'OTAN, dont une synthèse est fournie, puis précise les spécificités françaises. Le lecteur non spécialiste trouvera dans ce document les concepts, l'organisation et les principales capacités de la guerre électronique française. Il faut signaler l'ouverture qui y est faite vers une coordination plus poussée entre guerre électronique et cyberdéfense.

Du côté du site Intradef du Centre…

Depuis sa mise en ligne mi-juin, l'interface du nouveau site du CICDE s'est étoffée et ce dernier s'est enrichi des dernières parutions : doctrines, publications, synthèses de retour d'expérience, études prospectives stratégiques. Les planches synthétiques regroupant les corpus sont mises à jour régulièrement, au fur et à mesure de la mise en ligne des documents.

Les consultations de documents classifiés (DR-SF et supérieurs) sont désormais assujetties à une demande via l'adresse cicde.documentaliste.fct@intradef.gouv.fr.

Pour toute remarque, n'hésitez pas à contacter le webmestre du CICDE, qui s'efforcera de prendre en compte vos propositions d'amélioration.



Webmestre du CICDE : SGC Alice Rocquain (cicde.redaction-web.lst@intradef.gouv.fr ou PNIA : 821.753.4366).

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES ARMÉES

Directeur de la publication : Général de division Antoine WINDECK.
Rédacteur en chef : Colonel Jean-François LAGRANGE ☎ 01 44 42 83 43 • **Maquette** : Premier maître Philippe JEANVOINE ☎ 01 44 42 83 30 – Fax 01 44 42 82 72 • **Impression-Routage** : EDIACA-76, rue de la Talaudière-CS80508-42007 SAINT-ÉTIENNE cedex 1 ☎ 04 77 95 33 21 ou 04 77 33 25 • **Dépôt légal** : Décembre 2017 - ISSN en cours - Collection « Lettre du CICDE » •

Centre Interarmées de Concepts,
de Doctrines et d'Expérimentations

École militaire
1, place Joffre – BP 31
75700 PARIS SP 07

Site intradef : www.portail-cicde.intradef.gouv.fr