NOTE DE RECHERCHE PROSPECTIVE

FORUM de la pensée mili-terre

Armée de terre
Centre de doctrine et d'enseignement du commandement

Le renseignement d'intérêt militaire dans les *safe spheres*

Eva Micheletti
Rédactrice au pôle études et prospective

Ce document ne constitue pas une position officielle de l'armée de Terre.

L'enjeu de cette note est de montrer que les capacités d'appréhension et d'analyse de l'information seront au cœur des préoccupations futures pour le renseignement au sein de l'armée de Terre, dans un monde où il n'y aura potentiellement plus de perception commune de la réalité entre les individus.

Résumé du scénario de la saison 1 de la *Red Team* : « chronique d'une mort culturelle annoncée »

Les années 2020 voient le déploiement d'une nouvelle génération de réseaux de service, véritables bulles numériques communautaires : les « *safe spheres* ». Elles adaptent les perceptions du monde extérieur à la réalité que chacun veut lui donner. Les *safe spheres* sont des « réseaux communautaires qui se structurent autour de la profession, de la religion, de passions et convictions communes ou encore du quartier d'habitation ». « Elles ont pour objectif d'ajouter des éléments de réalité augmentée dans le champ perceptif, pour construire des réalités alternatives. Ces réalités sont variées. Certaines permettent une ludification du monde. D'autres ajoutent des éléments sacrés ou effacent des éléments susceptibles de heurter des sensibilités[1] ». Pour y accéder les individus se connectent aux *safe spheres* grâce à des lunettes de réalité augmentée, des inserts auriculaires ou des puces intradermiques[2]. En 2040, 90 % des européens y sont connectés si bien qu'il n'y a plus de réel commun partagé. Le 12 octobre 2045, un attentat biologique est commis au cœur de Grande-City, déjà touchée par une crue centennale. Quelques heures après l'armée française lance l'opération *Omanyd* pour rapatrier les ressortissants français. Les forces françaises arrivent dans un contexte de chaos climatique et d'alerte sanitaire au sein d'une population soumise à des réalités alternatives se révélant incapable « d'entendre » les

[1] *Red Team*, Chronique d'une mort culturelle annoncée, Saison 1.
[2] Entretien avec Marie Roussie, ingénieur de recherche à l'université Paris Sciences et Lettres, associée à la *Red Team.*

propos officiels. Entre le 14 et le 20 octobre 2045, l'armée française établit six points d'évacuation hors de Grande-City, mais de nombreux ressortissants s'opposent aux conditions d'évacuation voire se méfient des militaires. La critique médiatique est virulente, les *fake news* omniprésentes. Le 20 octobre 2045, les ressortissants sont rapatriés jusqu'à Voude avec une flottille de ferries mais ils se heurtent à des bateaux venus du continent qui s'opposent à l'arrivée des réfugiés par crainte de la contagion. Durant le mois de novembre 2045, l'arrivée des ressortissants en France obéit à un protocole strict. En 2047, l'opération « Sécuriser le Réel », sous mandat de l'Union européenne, est lancée pour contrôler les zones de réalités alternatives. En 2050, on estime qu'il faudra plusieurs années d'effort, pour désactiver les « *safe spheres* » les plus virulentes. Face à une balkanisation progressive du réel, comment retrouver le sens de l'intérêt général et d'un destin collectif ?[3]

Introduction. La guerre dans les « zones grises virtuelles ».

« La troisième guerre mondiale sera une guérilla de l'information, sans distinction entre la participation militaire et civile » (Marshall Mc Luhan, 1970).

Dans un environnement stratégique et tactique toujours incertain, le renseignement d'intérêt militaire (RIM) fournissant des informations utiles à la conduite des opérations de l'armée de Terre, est amené à évoluer pour s'adapter aux nouvelles technologies militaires et civiles. Cette note de recherche s'appuie sur les travaux de la *Red Team* et en particulier sur le scénario de la saison 1, « chronique d'une mort culturelle annoncée », qui introduit le concept de *safe spheres*[4]. Celui-ci décrit et imagine dans un futur proche, l'émergence de bulles informatiques virtuelles appelées *safe spheres.* Ce sont des « réseaux communautaires » qui ont pour objectif d'ajouter des éléments de réalité augmentée dans le champ perceptif, afin de construire des réalités alternatives. Elles s'intègrent dans le concept de métavers[5], défini comme un monde numérique perçu en réalité augmentée.

Dans ce futur imaginé, les citoyens sont soumis à des réalités parallèles et diverses, et par conséquent la perception du réel est très fragmentée. Si la plupart des *safe spheres* sont créées à des fins économiques, ludiques ou éducatives, on voit aussi apparaître dans ce scénario des *safe spheres* radicales, vecteurs de contestation cherchant à nuire et à paralyser l'action de l'armée française[6]. En ce sens, on peut parler de « zones grises virtuelles[7] ».

Il est important de noter que les stratégies dans les zones grises ont deux caractéristiques :

- elles visent à modifier l'équilibre des pouvoirs en faveur de l'agresseur ;
- elles sont conçues pour poursuivre cet objectif en évitant, estompant ou contournant les lignes rouges et l'escalade vers la guerre conventionnelle[8].

Dans le scénario, les forces armées n'ont pas accès à ces espaces numériques dissidents et évoluent dans leur *safe sphere* militaire dédiée, laquelle peut être fragmentée en communautés restreintes afin de contrer d'éventuels piratages[9].

---

[3] *Red Team*, vidéo de présentation du scénario « chronique d'une mort culturelle annoncée », https://redteamdefense.org/saison-1/chronique-dune-mort-culturelle-annoncee

[4] Voir résumé du scénario page 1.

[5] Entretien avec Marie Roussie, ingénieur de recherche à l'université Paris Science et Lettres, associée à la *Red team*.

[6] Voir résumé du scénario page 1.

[7] Le terme de zone grise signifie « un espace de dérégulation sociale, de nature politique ou socio-économique, échappant au contrôle de l'État » http://geoconfluences.ens-lyon.fr/glossaire/zones-grises

[8] Jake Harrington et Riley McCabe, "*Detect and Understand: Modernizing Intelligence for the Gray Zone*", CSIS, 7 décembre 2021.

[9] Red team, *op. cit.*

Au-delà du scénario de la *Red Team*, l'accélération de l'usage de ce type de technologies favorise en effet, à l'échelle mondiale, l'explosion et la diversification du volume et des flux de données, ainsi qu'une compétition accrue pour acquérir les outils de la suprématie numérique. Dans ce contexte, la gestion des données et de l'information constitue un enjeu crucial pour fournir un RIM efficient. Les institutions, les entreprises et les pays qui investissent dans des moyens d'acquérir, de classer, de monétiser et de stocker les données sont avantagés[10]. En outre, la notion de respect de la vie privée est totalement redéfinie car les individus partagent davantage d'informations personnelles afin d'accéder aux *safe spheres*.

Ceci renforce les gouvernements autoritaires qui continuent d'exploiter le *big data* pour surveiller et contrôler les populations. Le contrôle des données numériques devient un outil d'influence majeur. Des entreprises, organisations ou acteurs non étatiques disposent d'outils puissants pour manipuler l'information : vidéos truquées (*morphing, deep fake, face swap…*), utilisation de messages fabriqués par l'intelligence artificielle (IA). Les applications d'IA deviennent des cibles potentielles pour la manipulation des données. Dans le domaine cyber, la connectivité accrue des individus augmente la vulnérabilité des institutions : « la présence de centaines de milliards de dispositifs connectés accroit considérablement la surface d'attaque cyber-physique. En outre, l'application de la cyber sécurité fondée sur des frontières géographiques perd de sa pertinence dans un réseau de plus en plus international[11] ». Dans ce contexte, l'Europe et la France demeurent fragiles en matière de souveraineté numérique.

Après avoir mis en évidence l'enjeu crucial de l'accès et de la gestion de l'information de ces espaces virtuels, cette note aborde la façon, pour l'armée de Terre, de contrer les menaces ennemies en zones grises virtuelles.

1. <u>Localiser et analyser les menaces dans les zones grises virtuelles : l'enjeu de l'accès à l'information.</u>

Le volume d'informations et le rythme de diffusion de la menace en zone grise virtuelle augmentent de manière croissante, obligeant les forces terrestres à repenser le cycle du renseignement (orienter, rechercher, exploiter, diffuser). En effet, bien que produisant un plan de recherche très précis (avec le risque de passer à côté d'informations importantes), les agences de renseignement sont submergées par les données. D'ici 2025, le flux de données devrait être multiplié par deux pour atteindre 175 zettaoctets par seconde (soit 1 000 milliards de gigaoctets)[12].

Cette densification des données peut se répercuter jusqu'au système d'armes ou de commandement. Bénéficiant d'une réalité militaire augmentée, le soldat chargé de la recherche humaine peut se retrouver paralysé par une surcharge d'informations, en raison d'une saturation des données dans sa *safe sphere* dédiée.

Source : Modern War Institute

[10] Piotr Smolar, « Le Monde en 2040 vu par la CIA : Un monde plus contesté », Équateurs document, 28 avril 2021.
[11] *Ibid.*
[12] Jake Harrington et Riley McCabe, "*Keeping pace in the grey zone: three recommendations for the US intelligence community*", War on the rocks, février 2022.

Les nouveaux outils de renseignement des forces terrestres.

Il devient alors difficile de discriminer les vraies informations des leurres, de sélectionner les données à collecter. Le métavers offre également un formidable terrain de jeu pour l'adversaire, qu'il soit un combattant régulier ou irrégulier. La nécessité de sélectionner la donnée à récupérer (donc de la localiser, de la lire, de pouvoir la discriminer en temps réel et de pouvoir la transférer - peut être en temps différé), est alors la condition primordiale pour produire *in fine* un renseignement d'intérêt militaire pertinent, dans un univers où les perceptions du réel des individus sont biaisées. Les *safe spheres* peuvent être localisées grâce à l'analyse des connexions des utilisateurs et des données qui transitent, peut-être par une combinaison de guerre électronique et de cyberdéfense. « Un traitement *big data* colore cette couche plus ou moins fortement en fonction du flux de données qui y transite, la *safe sphere* est représentée comme étalée dans l'espace selon la géolocalisation de ses utilisateurs[13] ». À partir des métadonnées collectées, le scénario de la *Red Team* met en évidence la création d'une carte dynamique numérique. Ces cartes de plusieurs types (tactique, informationnelle, capacitaire, *etc*.) offrent de l'information de géolocalisation en continu, mais aussi des données, des idées, des rumeurs, *etc.*[14].

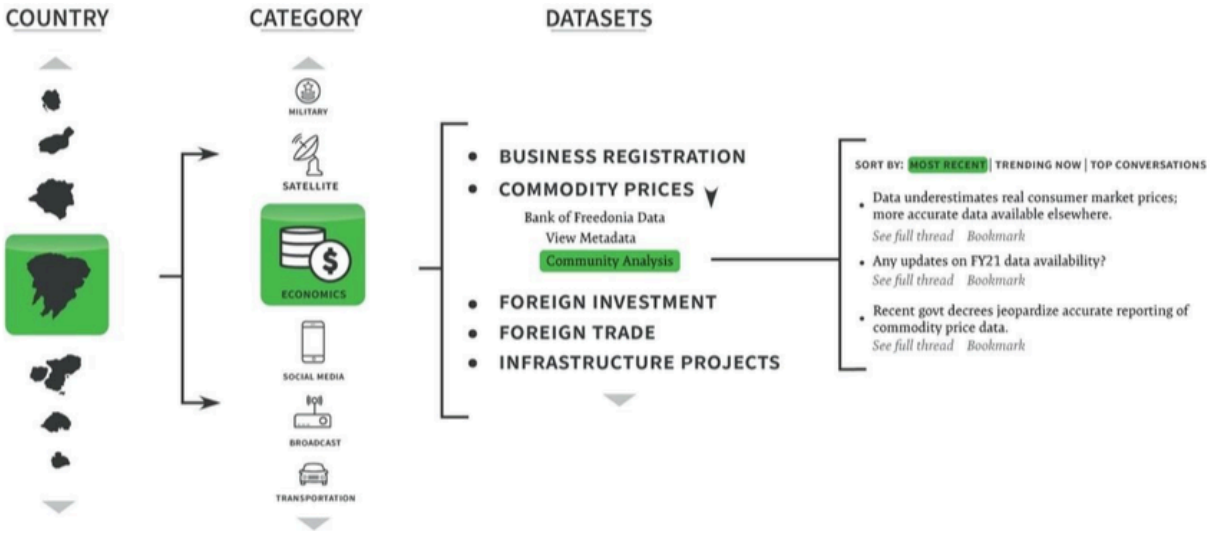
Les capacités et les outils à la disposition des forces terrestres pour collecter les données et caractériser les *safe spheres* pourraient être les suivants :

- la représentation topographique dynamique en 3D du terrain et des forces militaires en présence, sur laquelle seront plaquées les cartes[15] ;
- du renseignement et une manœuvre particulière pour couvrir la zone d'opération si les capacités automatiques ne permettent pas un recueil suffisant ;
- des drones et des robots avec leurs capteurs de la guerre de l'information (cyberdéfense et guerre électronique en particulier) ;
- des mini capteurs que les soldats ou les véhicules militaires transporteraient pour capter toutes les informations émises par les appareils numériques dans leur environnement proche (lunettes de réalité virtuelle, inserts auriculaires ou des puces intradermiques) ;
- des entrepôts tactiques de traitement de la donnée.

Le traitement massif des données sera plus que jamais le nerf de la guerre. Par conséquent, l'indépendance de l'armée Française en matière de gestion des données est primordiale. La recherche et l'exploitation d'informations pour le renseignement militaire dans un univers ultra-connecté nécessitent la possibilité de contrôler et de sécuriser les données propres aux forces terrestres. En ce sens la création d'un *cloud* souverain, défini comme : « *une infrastructure dans laquelle la puissance de calcul et le stockage sont gérés par des serveurs distants auxquels les usagers se connectent via une liaison Internet sécurisée. Les objets connectés deviennent des points d'accès pour exécuter des applications ou consulter des données qui sont hébergées sur les serveurs*[16] », permettrait une exploitation efficace d'informations massives et hétérogènes, en croisant des données brutes et des données structurées, offrant ainsi des « analyses multidimensionnelles sur la base de critères géographiques, temporels, relationnels ou statistiques[17] ».

[13] Red team, *op. cit.*
[14] Red team, *op. cit.*
[15] Red team, *op. cit.*
[16] https://www.futura sciences.com/tech/definitions/informatique-cloud-computing-11573/
[17] Laurent Lagneau, « Numérique : L'important projet ARTEMIS du ministère des Armées est-il trop ambitieux pour réussir ? », OPEX360, 9 novembre 2021.

Pour optimiser les transmissions dans un environnement de guerre souvent très abrasif, il peut être nécessaire d'avoir des entrepôts tactiques de données avec des capacités de traitement très déconcentrées. L'armée de Terre a donc un rôle important à jouer dans ce domaine. Le traitement des données comme pierre angulaire de l'analyse de l'information en zone de combat, et plus particulièrement en zone d'incertitude comme peut l'être la zone grise virtuelle, pourrait en outre reposer sur une orientation des capteurs facilitée par la création d'un catalogue de données de renseignement *open source* (OSINT), puisque les cibles ne seraient plus seulement militaires.



Représentation d'un hypothétique catalogue de données de renseignement open source, avec des ensembles de données organisés en catégories et accompagnés de perspectives analytiques générées par la communauté (source : programme de sécurité internationale du SCRS[18]).

La révolution du ROSO (renseignement d'origine sources ouvertes).

Les informations sur le champ de bataille circulent aujourd'hui massivement sur Internet (photo, vidéo, image satellite, informations dans les réseaux sociaux, et bientôt information dans les *safe spheres*). Le RIM doit ainsi s'appuyer sur des informations provenant d'internet et inclure la révolution du renseignement en *open source* grâce aux nouveaux outils numériques de qualification (pour éviter la manipulation) et de traitement de la donnée. En effet, les technologies fournissent « des données de capteurs à distance de plus en plus précises, des informations sur les cyber-menaces, des données sur les réseaux sociaux[19] ». Parce que les données sont en accès libre sur internet, l'analyse peut aussi être complétée par des productions issues d'intermédiaires de confiance comme des entreprises de type SMP ou cabinets de conseil spécialisés - *think tanks,* intégrées dans des plateformes participatives. Par exemple, la communauté du renseignement britannique s'appuie sur une plateforme qui intègre les prévisions d'un large panel d'experts gouvernementaux et non gouvernementaux de confiance, baptisée *Cosmic Bazaar*. « L'utilité potentielle de ces plateformes participatives ne fera que croitre à mesure que la qualité et le détail des données disponibles pour les analystes non gouvernementaux augmenteront. S'il existe un consensus sur le fait que l'intelligence *open source* sera un perturbateur à l'avenir, les personnes et les organisations qui analysent ces données - les universités, les organisations non gouvernementales et le secteur privé - doivent être intégrées en tant que partenaires[20] ».

[18] Jake Harrington et Riley McCabe, *op. cit.*
[19] *Ibid.*
[20] Jake Harrington et Riley McCabe, *op. cit.*

2. Contrer les menaces ennemies en zones grises virtuelles.

La guerre de l'information peut être définie comme une « manipulation ou utilisation délibérée d'informations par une partie sur un adversaire pour influencer les choix et les décisions que l'adversaire prend à des fins militaires ou stratégiques[21] ». Elle s'appuie sur les opérations dans le cyberespace, la guerre électronique, les opérations psychologiques, la sécurité des opérations. Elle contribue donc pleinement au RIM dans les *safe spheres*. En effet, les groupes extrémistes présents dans des *safe spheres* ne respecteront pas les règles d'engagement conventionnelles, ils y feront usage de stratégies de désinformation de masse, de leurres sensoriels, d'hologrammes, de piratage de réseaux de communication ou de constitution de micro-zones blanches[22]. Le renseignement d'intérêt militaire dans les zones grises virtuelles devra ainsi prendre en compte :

- l'identification et l'attribution des indicateurs d'activités hostiles pour pouvoir repérer les opérations de guerre de l'information et les comportements inhabituels sur lesquels se porteront un effort de captation de données (détecter) ;
- la contextualisation, dans une compréhension plus large, de la stratégie et des intentions de l'ennemi (comprendre)[23].

Le ROHUM dans les *safe spheres*.

Un des enjeux essentiels de la collecte du renseignement réside dans l'accès à cette zone grise virtuelle. Cela nécessite un accès direct à l'univers de la *safe sphere,* mais dans certains cas, celui-ci s'avère périlleux en raison d'une hostilité des usagers aux forces armées et des mesures de protections de cyberdéfense. Dans cette optique, il faut envisager le recours à des modes d'action « traditionnels » renseignement d'origine humaine (ROHUM), en particulier du « renseignement de contre-insurrection ». Infiltrer les *safe spheres* pourrait être possible grâce au déploiement de capteurs humains de renseignement dans un monde virtuel, tels que des avatars contrôlés par des agents infiltrés. En effet, à l'image des réseaux de résistance *Gladio* après la Seconde Guerre mondiale en Italie, dont le principe est repris par les forces spéciales américaines actuellement, le *Resistance Operating Concept* (ROC)[24] pourrait être retranscrit au sein de réalités virtuelles. Ce concept fait le pont entre guerre non conventionnelle et résistance. Cette initiative est fondée sur le renforcement de la capacité d'entités alliées (par exemple dans le cas présent un réseaux d'agents clandestins infiltrés dans une *safe sphere*) à monter une résistance militaire efficace s'ils devaient faire face à l'invasion et à l'occupation par une puissance hostile (État autoritaire ou firmes du numérique) contrôlant la gestion des *safe spheres*. Selon le colonel Christopher Stangle, commandant le 4e groupe d'opérations psychologiques au sein de l'US Army : « *mettre en place les conditions d'une*

Source : Red Team Defense.

[21] T. Sanders, "*New Zealand Chief of Army Writing Competition Winner of the Civilian Category: The Impact Information Can Have on the NZ Army in the Contemporary Battlespace of Information Warfare"*, Knowledge enable army,16 décembre 2021.
[22] Red team, *op. cit.* Les zones blanches sont des zones géographiques non desservies par les réseaux de communication.
[23] Jake Harrington et Riley McCabe, *op. cit.*
[24] Davis Winkie, "*Less door-kicking, more resistance: Inside Army SOF's return to unconventional warfare*", Defense news, 9 septembre 2021.

défense et d'une résistance totales nécessite d'obtenir et de maintenir le soutien de la population civile en la « vaccinant et en la durcissant » contre la désinformation ennemie[25] ». Ainsi, la collecte d'information va de pair avec des logiques d'influence et de contre-espionnage. En réponse aux actions de sabotage ennemies, la déception, englobant la dissimulation et la simulation, passerait par le repérage et l'analyse du discours des relais d'opinions ennemis et l'intoxication des médias et supports d'informations virtuels. Il s'agit donc de mener une guerre irrégulière sur le territoire ennemi et d'être, selon le colonel Stangle, « *réactif à la désinformation de l'adversaire* ». La tâche n'est cependant pas aisée : « *Vous devez visualiser ce que l'adversaire va utiliser contre vous, puis saper ces points négatifs dès le départ et supprimer ces arguments afin qu'ils ne puissent pas être utilisés contre vous*[26] ».

La matérialité de la *safe sphere* n'est pas à négliger. Dans le domaine des réseaux informatiques, la couche physique est la première couche du modèle OSI (*Open Systems Interconnection*, « Interconnexion de systèmes ouverts »). Elle est chargée de la transmission effective des signaux électriques, radiofréquences ou optiques entre les interlocuteurs[27]. Cette couche physique est composée d'équipements électroniques dont l'ingénierie et la construction nous échappent. Aujourd'hui la Chine contrôle en grande partie la chaine d'approvisionnement et de production des outils numériques. Elle bénéficie donc d'un avantage dans la guerre de l'information car elle dispose d'un accès privilégié à cette couche physique par des opérations de cyberdéfense.

Conclusion.

Outre l'infiltration directe au sein des *safe spheres*, il s'agit aussi pour le renseignement militaire de neutraliser et de contrer les actions des usagers hostiles en agissant dans le domaine cyber sur les infrastructures numériques qui hébergent les *safe spheres.* Dans une perspective future, l'enjeu primordial sera d'identifier qui contrôle ces réseaux de communication en réalité augmentée et où ils seront physiquement installés (sous quelle autorité étatique et quelle législation). Dans une première hypothèse, les données sont stockées dans des *data center* très protégés : la cible hébergeant les données des *safe spheres* serait alors clairement identifiable et pourrait faire l'objet d'attaques cyber. Cependant, selon Guillaume Pitron[28], d'ici 2025, 80 % des institutions et des entreprises auront délaissé les *data center* tels qu'on les connaît aujourd'hui. La seconde hypothèse imagine que les outils de stockage abritant les données des *safe spheres,* ou applications équivalentes, sont livrés aux particuliers par les grandes entreprises (futures GAFAM). Le système de répartition de pair à pair, comme pour les *darkweb* et *deepweb,* sera aussi très certainement utilisé comme il l'est aujourd'hui pour d'autres usages. On peut alors imaginer un système de *box* qui stocke l'ensemble des données propres à la *safe sphere* du particulier. Ce dernier peut personnaliser l'ensemble du contenu qu'il partage avec une communauté, qu'il pourra influencer à travers cette déclinaison de l'outil *safe sphere* initial.

En considérant ces modes de stockage, la destruction des *safe spheres* devra alors passer par une opération combinée d'actions physiques, d'actions de cyberdéfense, probablement de guerre électronique, mais aussi d'influence.

[25] *Ibid.*
[26] Davis Winkie, *op. cit.*
[27] https://fr.wikipedia.org/wiki/Couche_physique
[28] Guillaume Pitron, « L'enfer numérique. Voyage au bout d'un Like », Les Liens qui Libèrent, septembre 2021, 304 p.