Désinformation et manipulation, quelles réponses françaises dans le champ informationnel ?

Loïc Girard

Colonel (terre), auditeur de la 69e session du CHEM.

« L'homme est bâti de manière que les fictions font beaucoup plus d'impression sur lui que la vérité. »
Érasme, *Éloge de la folie* (1511).

Fort du postulat énoncé par Érasme, Napoléon Ier a su s'appuyer sur les bulletins de la Grande Armée pour toujours donner plus d'éclat à ses actions. Il choisissait les victoires pour le servir au temps de sa gloire [1] – entretenir le mythe de son invincibilité auprès des Français et de ses ennemis – comme pour tenter de ralentir l'inéluctable lors des dernières campagnes à la fin de son règne [2]. Ce postulat – la nature humaine, terreau réceptif à la désinformation – prend une acuité particulière aujourd'hui compte tenu des évolutions récentes et rapides ces dernières années dans le champ informationnel.

La désinformation et la manipulation de l'information ont toujours existé, dans le domaine militaire comme dans le monde civil. Mais le contexte, les outils disponibles, les conditions de cette transformation et les acteurs majeurs ont singulièrement évolué au point d'en bouleverser les règles et d'augmenter sans commune mesure les risques et les menaces que la manipulation de l'information fait peser sur nous.

Compte tenu de ces évolutions, il est désormais admis que le champ informationnel est un sixième milieu [3], espace dans lequel évoluent librement l'information de toute nature et les nombreux acteurs concernés, qu'ils soient émetteurs ou cibles de cette information utilisée comme moyen ou comme arme. Les actions dans cet espace de confrontation se déclinent ainsi en un large spectre qui va de la stratégie d'influence – y compris celle de nos alliés – à la volonté de déstabilisation d'un compétiteur stratégique. Parmi les nombreux acteurs, les États et les plateformes numériques [4] occupent une position centrale, d'autant plus pour ces dernières qui sont à la fois

[1] Il a ainsi donné un relief particulier à la bataille d'Iéna qu'il remporta en 1806 pour éclipser la victoire du maréchal Davout pourtant plus déterminante à Auerstaedt au même moment.
[2] « Il commença par rédiger le premier bulletin de la Grande Armée depuis l'entrée en campagne (…). Les nouvelles (…) étaient mauvaises (…). Il était urgent de rendre à la réalité ses justes proportions et de faire valoir les raisons d'espérer. » Bernard Michel, *Hiver 1814, campagne de France*, Perrin, 2019, p. 65.
[3] Les milieux ainsi définis : Terre, air, mer, espace, cyber et champ informationnel.
[4] Toutes les sociétés dont les réseaux sociaux sont la ou une raison d'être.

acteurs et vecteurs. S'y ajoutent toutes les organisations ayant des intérêts à défendre ou à contester parmi lesquelles les groupes politiques radicaux ou alternatifs et les entités terroristes.

Dans ce contexte, les démocraties libérales sont, par nature, particulièrement exposées à la manipulation de l'information, non seulement par leur ouverture politique mais aussi parce qu'elles ne peuvent user des mêmes armes pour s'en défendre. C'est aussi un domaine qui peut être considéré soit isolément – ce qui sera le cas dans la présente réflexion –, soit mêlé à d'autres dans le cadre des menaces hybrides [5] ou de la superposition des milieux et des réponses multidomaines à y apporter.

La désinformation exploite nos fragilités, conteste et mine notre modèle de société, c'est un fait. Il convient donc de s'en prémunir à tous les échelons de l'État tout en développant plus avant notre propre stratégie d'influence. Nous avons donc besoin de nous doter des doctrines, organisations et moyens capables de veiller, de nous défendre et d'agir dans cet espace de confrontation, en particulier pour nos opérations militaires. En s'assurant de la légalité des actions conduites, la désinformation doit nous faire repenser l'influence notamment *via* la priorité à accorder à la communication stratégique (*StratCom*) [6], entendue comme la mise en cohérence et la coordination des messages avec les actions au service d'une stratégie.

Il sera tout d'abord question de rappeler le contexte et les enjeux afin de prendre conscience combien ces derniers sont déterminants. Il s'agira ensuite de mesurer les menaces dont nous faisons l'objet au regard des décisions prises par nos alliés pour y faire face. Un panorama des actions déjà entreprises en France et de celles qui pourraient être conduites sera enfin effectué, notamment le besoin de repenser la *StratCom* et de lui accorder une place originelle dans les opérations militaires.

Un contexte perméable aux capacités accrues du champ informationnel

Le contexte est connu mais il convient de le rappeler brièvement. L'exemple français est à ce titre significatif à bien des égards : une société fragmentée [7] pouvant aller vers de nouvelles contestations [8], une moindre confiance dans la parole publique avec une forme de relativisme généralisé et *in fine* une désaffection progressive des urnes qui affaiblit la légitimité du pouvoir. Compte tenu de cette période de fragilité et de remise en cause au sein des démocraties libérales, notre population est, par conséquent, davantage exposée voire réceptive aux manipulations de l'information.

---

[5] La menace hybride est une forme ambiguë d'affrontement combinant les actions militaires conventionnelles et non conventionnelles ainsi que des actions non militaires fondées sur une stratégie de déstabilisation de l'adversaire.

[6] Afin d'éviter le mélange de genre avec la communication, l'expression *StratCom* s'est vue préférée pendant longtemps à celle de stratégie d'influence : cela n'a fait que renforcer l'inhibition à l'utiliser, compte tenu de la connotation du terme et de ses interprétations possibles.

[7] Fragmentation que l'on retrouve théorisée de manière complémentaire dans des ouvrages au fort retentissement comme *La France périphérique* de Christophe Guilluy (2014) et *L'Archipel français* de Jérôme Fourquet (2019).

[8] *Black Blocs*, Gilets jaunes, altermondialistes radicaux, etc.

Ce phénomène est décuplé par l'évolution majeure que constitue la transformation numérique à l'œuvre et qui permet à la fois la vitesse de propagation et l'individualisation de l'information [9]. *Internet* et les réseaux sociaux permettent ainsi d'adapter le message à chaque individu. Cela offre un champ des possibles qui repousse les limites connues grâce à la technologie et à l'intelligence artificielle (IA). Par exemple, la production de vidéos falsifiées – les *Deep Fake* – nécessitait, jusqu'à présent, des moyens spécialisés pour être techniquement au point [10]. Elle devrait être accessible dans quelques années *via* des applications grand public.

Les États, acteurs majeurs du champ informationnel

Les acteurs et leurs modes d'action enfin sont des éléments essentiels au sens où ils participent à remodeler en permanence ce paysage. De nombreux États occupent cet espace avec un objectif aussi clair que rarement assumé qui se traduit par « l'affirmation de plus en plus nette de stratégies de puissance ayant recours sans remords à des stratégies digitales de déstabilisation qui s'exercent dans le champ informationnel » [11].

La première règle qui s'applique dans le champ informationnel pour un acteur est la défense de ses intérêts à laquelle s'ajoutent les limites qu'il veut bien se fixer, parfois jusqu'à une politique délibérément hostile. Dans ce large spectre d'actions possibles, les moyens utilisés sont très vastes. Les *Fake News* sont les plus « simples » à identifier si l'on se réfère à la définition qui en est faite : « article qui est intentionnellement faux et de manière vérifiable » [12]. Il est le plus souvent difficile d'identifier un acte malveillant, la désinformation étant souvent bâtie selon la méthode du 80-20-10 qui mêle un peu de faux à beaucoup de vrai : « une fausse nouvelle est construite de 80 % d'histoires empiriquement vraies, 20 % de contenus défendables bien que contestés et 10 % de faits sans fondement véridique (dépasse 100 % car les périmètres ne sont pas disjoints) » [13]. Ensuite, la technique peut aussi masquer tout ou partie de son origine. Enfin, la collusion possible d'intérêts convergents complique la tâche en brouillant la source initiale. Il semble ainsi avéré que l'affaire dite des *Macron Leaks* aurait combiné l'action des services russes et celle de la droite alternative américaine [14]. L'attribution est par conséquent souvent compliquée.

En outre, compte tenu de « la nature transnationale d'un phénomène qui se joue des cadres de la souveraineté » [15], il est compliqué de défendre une frontière ou

---

[9] Le ciblage de l'individu serait plus juste.

[10] Un célèbre *Deep Fake* de l'ancien président Obama a été réalisé à but pédagogique en 2018 (https://m.youtube.com/) quand un autre de Nancy Pelosi, présidente démocrate de la Chambre des représentants a, lui, été réalisé pour nuire (www.youtube.com/watch?v=sDOo5nDJwgA).

[11] Le Drian Jean-Yves, « Discours de clôture de la conférence internationale "Sociétés civiles, médias et pouvoirs publics : les démocraties face aux manipulations de l'information" », Paris, 4 avril 2018 (www.diplomatie.gouv.fr).

[12] Levasseur Guillaume, *Mise en perspective stratégique des techniques numériques émergentes de falsification des informations sur* Internet (thèse professionnelle de master spécialisé), Telecom ParisTech, novembre 2018, p. 22.

[13] *Ibid.*, p. 38.

[14] Jeangene Vilmer Jean-Baptiste, *The « Macron Leaks » Operation: A post-Mortem*, Atlantic Council-Irsem, juin 2019, p. 23 (www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf).

[15] Jeangene Vilmer Jean-Baptiste, Escorcia Alexandre, Guillaume Marine et Herrera Janaina, *Les Manipulations de l'information*, Caps-Irsem, août 2018, p. 8 (www.diplomatie.gouv.fr/).

un territoire dans le champ informationnel. La porosité des milieux est une caractéristique essentielle de ce domaine : entre ce qui se passe sur le territoire national et ce qui vient de l'étranger, entre ce qui relève du civil et du militaire, entre la manipulation de l'information avérée et ce qui peut ou doit être considéré comme une opinion politique enfin – difficulté entre toutes dans ce dernier cas, cette porosité contribue à brouiller le paysage et à compliquer les réponses à apporter.

Les plateformes numériques, des sources potentielles de déstabilisation démocratique

Les plateformes numériques privées et leurs réseaux sociaux sont, par construction, les vecteurs sans limite apparente d'un nombre phénoménal et croissant d'informations [(16)]. Elles disposent d'une force de frappe financière sans équivalent – une capitalisation boursière correspondant au PIB d'un État [(17)]. Elles ont une indépendance de fait doublée d'une volonté revendiquée de « changer le monde » [(18)] sans contrôle, ni de régulation *a minima*. Elles sont animées par la recherche du profit *via* l'usage des données individuelles à des fins commerciales. Si on ajoute à cela que les autres acteurs malintentionnés non cités s'appuient aussi sur leurs réseaux pour manipuler l'information, elles représentent donc une partie du problème et de la solution. La crise du Covid-19 devrait accroître encore davantage leur pouvoir [(19)], ce qui n'a rien de rassurant.

Leur responsabilité est donc engagée dans la transmission des informations et dans la gestion des données privées. Elles sont tout d'abord responsables *a posteriori* de l'information – la désinformation en l'occurrence – qu'elles laissent véhiculer sur leur réseau. De leur capacité de détection en propre, de leur rapidité de réaction, notamment à nos sollicitations, et surtout de leur volonté d'agir dépend en grande partie l'efficacité de la lutte contre la manipulation de l'information.

Enfin, par les données qu'elles détiennent et qu'elles sont censées protéger, et l'usage qu'elles en font de manière opaque, ces plateformes font aussi peser un risque sur notre modèle démocratique. Les exemples récents de dérives ou d'actions malveillantes visant à influencer le débat démocratique ou à déstabiliser les élections et les impliquant sont ainsi significatifs. Ce fut le cas en 2016, à la fois pour l'élection du Président américain et pour la campagne du *Brexit* au Royaume-Uni par l'intermédiaire

---

(16) Le président Macron a réuni 36 millions de téléspectateurs le 16 mars 2020 pour ses annonces liées à la crise du Coronavirus – record absolu à la télévision, à mettre en perspective avec les plus de 26 M de visiteurs uniques sur Facebook en France tous les jours en moyenne (avant la crise du Covid-19).

(17) Quand la capitalisation de Facebook évolue autour des 600 milliards de dollars, cela la situe entre le PIB de la Turquie et celui de Taïwan, soit au 20e rang mondial environ.

(18) Mark Zuckerberg dans un discours de 2014 : « Facebook s'est donné pour mission de rendre le monde plus ouvert et plus connecté » ou le portait fait de lui dans un article du *New Yorker* le 13 septembre 2010 de José Antonio Vargas, le décrivant comme se référant depuis des années déjà à *L'Énéide* et sa volonté de « bâtir un empire sans frontière ». Duneau Clémence, « Facebook : comment le discours de Mark Zuckerberg a changé en quatorze ans », *Le Monde*, 11 avril 2018 (www.lemonde.fr/).

(19) « Il y a un incontestable effet d'aubaine pour les grandes plateformes numériques. Ce sont elles qui assurent aujourd'hui les connexions entre pays, individus et organisations. Elles façonnent les rapports politiques et sociaux. Elles sont désormais au cœur des rapports de puissance. » Semo Marc, « Thomas Gomart : "La crise due au coronavirus est la première d'un monde *post*-américain" », *Le Monde*, 8 avril 2020.

de la société Cambridge Analytica et du scandale éponyme [20]. Dans les deux cas, il était question de dérives antidémocratiques *via* l'usage dévoyé des données individuelles détenues par Facebook.

Les militaires, une cible privilégiée

Le militaire engagé en opérations n'est pas protégé de ces menaces, bien au contraire. Les récents conflits en Crimée puis au Donbass l'ont durement rappelé aux unités ukrainiennes en 2014 et en 2015 [21]. Ce n'est pas une nouvelle menace, mais elle est devenue extrêmement dangereuse en raison du développement fulgurant des moyens technologiques. Nos troupes en opérations font l'objet également de campagnes de dénigrement dont les effets sont souvent recherchés dans la durée. Ce fut le cas en République centrafricaine. C'est encore le cas au Mali contre la France, en général et l'opération *Barkhane*, en particulier [22]. Au-delà de l'indispensable protection, le militaire doit être capable d'adopter une posture proactive, ce que la ministre des Armées [23] intègre quand elle énonce : « la guerre de demain, c'est aussi une guerre d'influence et de désinformation auprès des populations ».

Pourtant, comme c'est le cas avec l'approche indirecte de la guerre, le militaire français n'a jamais été vraiment à l'aise avec l'information comme vecteur d'influence. « Guerre juste » catholique, modèle de la chevalerie, messianisme moral des Lumières, esprit cartésien, cet héritage mêlé n'est pas sans parfois inhiber nos actions dans ce champ et nous incline à préférer spontanément une approche directe de la guerre : « Notre tradition historique explique sans doute pour une bonne part cette réticence à utiliser ces armes du *Soft Power* [24]. Pour le dire plus crûment, nous nous méfions des manœuvres qui ne sont pas parfaitement visibles (…). Nous avons la perpétuelle tentation de l'efficacité immédiate qui passe par le choc direct. Pour preuve nos combats héroïques mais difficiles d'août 1914. On fait fi du renseignement, on croit que l'on va créer la surprise, on préfère agir en fondant sur l'adversaire, en croyant benoîtement que la *furia francese* suffira à l'emporter. [25] ». Théoricien de la stratégie indirecte, Liddell Hart le résume, quant à lui, de manière lapidaire quand il parle de la « doctrine simpliste de Foch [26] ». Nous avons connu néanmoins de manière cyclique quelques beaux succès dans ce domaine. La stratégie d'influence du général de Lattre en Indochine en 1950-1951 a ainsi été une parenthèse brillante [27] grâce à son implication

---

[20] Voir le documentaire très complet « The Great Hack : l'affaire Cambridge Analytica », Netflix (2019), ou le récent ouvrage *Mindfuck* de Christophe Wylie paru en mars 2020 chez Grasset.

[21] Tenenbaum Élie, *Partisans et centurions, une histoire de la guerre irrégulière au XXe siècle*, Perrin, 2018, p. 412.

[22] Exemple emblématique relaté par la cellule *fact checking* de l'*AFP*, quand le don de motos aux forces armées maliennes par les militaires de l'opération *Barkhane* est détourné en livraison aux terroristes : Faivre Le Cadre Anne-Sophie, « Non, l'armée française n'a pas livré des motos à des jihadistes au Mali », *AFP*, 4 décembre 2019 (https://factuel.afp.com/non-larmee-francaise-na-pas-livre-des-motos-des-jihadistes-au-mali).

[23] Parly Florence, « Discours de la ministre des Armées de clôture de l'université d'été de la Défense », Avord, 13 septembre 2019 (www.vie-publique.fr/discours/270451-florence-parly-13092019-politique-de-defense).

[24] Nye Joseph S., *The Means to Success in World Politics,* Public Affairs, 2004, 208 pages.

[25] Desportes Vincent, « Opérations extérieures et opérations d'influence », *Communication & Influence*, n° 40, janvier 2013 (www.comes-communication.com/).

[26] Liddell Hart Basil H., *Stratégie*, Perrin, 2017 (édition originale 1954), p. 528.

[27] Planchais Jean, « À la rubrique défense du journal *Le Monde* 1945-1965 », *in* Forcade Olivier, Duhamel Éric et Vial Philippe (dir.), *Militaires en République 1870-1962*, Publications de La Sorbonne, 1999, p. 536-537.

personnelle et à l'accent mis sur la lutte des idées dans un contexte de guerre froide. L'influence a aussi été déterminante dans l'école française de contre-insurrection. Toutefois la fin de cette période en 1962 a indistinctement mêlé oubli et opprobre sur les réflexions et travaux conduits jusqu'alors. Ce chapitre fermé, quelques tentatives ont pu survenir depuis, mais c'est bien à la faveur des évolutions récentes et de la prise de conscience des dangers encourus qu'il a été rouvert.

Des menaces qui évoluent rapidement

Le contexte et les enjeux ayant été rappelés, il s'agit maintenant de revenir tout d'abord sur la menace pour l'illustrer et de voir ensuite comment nos alliés y font face. C'est une source riche d'inspiration pour nous dans un champ qui évolue rapidement.

La Russie, menace la plus immédiate… mais pas la plus dangereuse sur le long terme

La Russie reste aujourd'hui l'acteur emblématique du domaine. C'est l'héritage laissé par l'Union soviétique comme par une doctrine toujours assumée dans le champ militaire. Les médias comme *Russia Today* et surtout *Sputnik* sont passés maîtres dans l'art d'amplifier les informations agressives (Gilets jaunes par exemple) ou de relayer des informations biaisées [(28)]. Elle pratique également l'ingérence extérieure comme celle dont fut victime la campagne présidentielle française lors de l'affaire des *Macron Leaks*. La « doctrine Gérasimov », quant à elle, stratégie de défense nationale dévoilée en 2015 [(29)], intègre l'information tantôt comme un « champ de bataille » tantôt comme une « arme », dans une logique de contre-offensive face à la guerre hybride dont la Russie serait victime de la part des Occidentaux en général, des Anglo-Saxons en particulier. De nombreuses manipulations d'information sont, par conséquent, attribuées à la Russie par les États-Unis, la Grande-Bretagne et l'Otan en particulier, mais également par l'Union européenne. Il est ainsi significatif que la Russie soit accusée par l'UE de profiter de la crise du Coronavirus pour affaiblir les pays occidentaux comme une dépêche *Reuters* du 18 mars 2020 s'en fait officiellement l'écho [(30)]. Cependant son action ne s'arrête pas aux frontières de l'Europe. Elle est aussi active à l'encontre de la présence française là où nos troupes sont engagées en Afrique [(31)]. Elle ne cherche pas à proposer un modèle alternatif ou à promouvoir une idéologie comme ce fut le cas lors de la guerre froide. Tout au plus conforte-t-elle son image autoritaire. Son mode d'action se fonde principalement sur la nuisance et le travail de sape pour déstabiliser dans la durée. Aussi active et visible soit-elle, son action ne doit pas occulter

---

(28) *AFP*, « À Versailles, Macron a parlé *cash* à Poutine sur la Syrie, les Droits de l'Homme ou les médias russes », *La Croix*, 30 mai 2017 (www.la-croix.com/).

(29) Facon Isabelle, « La nouvelle Stratégie de sécurité nationale de la Fédération de Russie (présentation analytique) », *Note de la FRS* n° 05/2016, Fondation pour la recherche stratégique, 10 février 2016 (www.frstrategie.org/).
Marangé Céline, « Les stratégies et les pratiques d'influence de la Russie », *Étude de l'Irsem*, n° 49, mars 2017, Institut de recherche stratégique de l'École militaire (www.defense.gouv.fr/).

(30) « *Russian media have deployed a 'significant disinformation campaign' against the West to worsen the impact of the coronavirus, generate panic and sow distrust, according to a European Union document* ». Emmott Robin, « Russia deploying coronavirus disinformation to sow panic in West, EU document says », *Reuters*, 18 mars 2020 (www.reuters.com/).

(31) Faivre Le Cadre Anne-Sophie, *op. cit*.

la multiplicité des acteurs qui manipulent l'information à des degrés divers dans cet espace de conflictualité. Ce serait donc un tort de ne suivre que la seule Russie.

À ce titre, il est instructif de constater les efforts déployés tous azimuts par la Chine pour faire croire qu'elle contrôle la situation s'agissant de la crise du Coronavirus avec un succès mitigé à ce jour [32]. Le narratif chinois est différent du russe au sens où il promeut clairement un modèle [33], en plus de s'attaquer à celui de ses compétiteurs stratégiques, américains en particulier. Il est activement à l'œuvre par les réseaux sociaux occidentaux tout d'abord. Il est ensuite conduit de manière plus traditionnelle vers tous les autres pays où elle estime son influence déterminante au regard de son implantation locale ou de son projet de route de la soie. Ainsi, cette une du journal togolais *L'Union* en date du 13 mars 2020 [34] qui titre « Baisse drastique des contaminations et hausse des guérisons » en Chine avec l'*interview* de l'ambassadeur chinois. Il est question ensuite de « mesures idoines prises par les autorités » chinoises mais aussi de dons de la Chine à l'Union africaine alors que dans le même temps « l'épidémie s'étend rapidement en Europe ». Cet exemple se multiplie à l'envi dans la presse des autres pays d'Afrique. S'il n'y avait les *tweets* du président Donald Trump, lequel s'évertue à parler de *Chinese virus*, la Chine pourrait presque réussir à faire oublier qu'elle est le premier foyer du virus mais encore plus gravement de la crise qui en découle. Quand les réseaux sociaux sont des vecteurs à leur insu de la lutte contre la désinformation !

Chez nos alliés, une priorité claire à la prise en compte de cet espace de conflictualité

Les interventions du Président américain sont d'ailleurs dans la droite ligne offensive de la politique que les États-Unis mènent dans ce domaine dorénavant. Tirant les enseignements des difficultés rencontrées par leur *StratCom* depuis plusieurs années et de leur fragilité politique dont le point d'orgue a été l'élection présidentielle de 2016, ils ont considérablement revu leur doctrine et leurs moyens. S'appuyant sur des actions cyber offensives, ils déclinent maintenant officiellement un concept appelé *Defense Forward and Persistent Engagement* [35] qui ne laisse aucun doute sur leurs intentions : neutraliser un adversaire potentiel de manière préventive dans ces nouveaux champs de conflictualité. Ils l'auraient d'ailleurs mis en œuvre pour protéger les dernières élections de mi-mandat [36]. Sous l'impulsion de leur précédent chef d'état-major des armées, le général du Corps des *Marines* Joseph Dunford, l'information a aussi été érigée en 7e fonction interarmées au même titre que le renseignement, le mouvement et la manœuvre ou les feux par exemple dans la continuité de leur concept *Multi*

---

[32] « Les autorités chinoises se mobilisent comme jamais pour faire croire que ce serait la Chine, la gagnante, afin de justifier leur modèle politique non seulement à l'intérieur mais désormais à l'extérieur, et leur discours a viré à une propagande caricaturale. » Gomart Thomas, *op. cit*.

[33] La propagande n'est pas exclue de ce narratif.

[34] *L'Union*, n° 1317, 13 mars 2020 (www.republicoftogo.com/).

[35] « *Defending forward as close as possible to the origin of adversary activity extends our reach to expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins.* », extrait de la *Command Vision for US Cyber Command*, février 2018, p. 6.

[36] Pomerleau Mark, « Two years in, how has a new strategy changed cyber operations? », *FifthDomain*, 11 novembre 2019 (www.fifthdomain.com/).

Domain Operations (*MDO*) [37]. Après une phase d'études approfondie, les futurs documents de doctrine à paraître [38] devraient profondément remanier les processus de décision et la conduite des opérations en élaborant des manœuvres au profit de l'information et non l'inverse. Pendant de cette approche offensive, les Américains mènent une politique affirmée d'attribution dès lors qu'ils identifient la désinformation selon le principe du *name and shame*.

Forts d'une tradition bien établie, les Britanniques sont, de leur côté, très avancés sur le sujet. Une transformation ambitieuse appelée *Information Advantage* [39] est en cours, lancée par le *Ministry of Defence* (*MoD*) en 2018 dans une logique interministérielle. Chaque armée a développé sa propre structure, par exemple la création de la 6e Division de l'*Army* qui regroupe tous ses moyens d'action dans les champs immatériels. Des efforts significatifs sont également conduits pour s'assurer que cette évolution est bien prise en compte dans l'ensemble des organismes et pour former les officiers à ces questions. Le *Joint Information Activities Group* est ainsi l'un des plus gros centres de formation à l'influence militaire en Europe. Les Britanniques, comme les Américains, attribuent également officiellement l'origine de la désinformation qu'ils identifient.

Les Allemands, quant à eux, ont principalement porté leurs efforts sur l'organisation. Ils ont ainsi décidé, en 2017, de créer une « 6e armée » qui regroupe les capacités stratégiques liées au renseignement, au cyber, à l'information, aux Systèmes d'information et de communication (SIC), à la guerre électronique et au spatial au sein du *Cyber und Informations Raum* (*CIR*) [40]. Il est encore un peu tôt pour savoir quels résultats ont été obtenus suite à cette réorganisation d'ampleur unique en son genre. Quoi qu'il en soit, l'Allemagne conserve une expertise technique de haut niveau dans tous ces domaines, aussi reconnue que limitée en termes d'actions possibles par leurs règles constitutionnelles.

Dans la continuité, l'Otan a réussi à dépasser une approche classique des médias en s'accordant sur une politique militaire liée à la *StratCom* en 2017 [41] et en créant des instances dédiées : le Centre d'excellence pour la communication stratégique à Riga [42] puis le Centre d'excellence européen pour la lutte contre les menaces hybrides avec l'UE à Helsinki [43]. L'influence active des États-Unis, de la Grande-Bretagne, de

---

[37] « *The U.S. Army in Multi-Domain Operations 2028 concept proposes series of solutions to solve the problem of layered standoff. The central idea in solving this problem is the rapid and continuous integration of all domains of warfare (…)* ». United States Army Training and Doctrine (TRADOC), *The US Army in Multi-Domain Operations 2028*, 6 décembre 2018 (www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf).

[38] Sur la base de ces études, un premier concept a été publié en juillet 2018 : *Joint Concept for Operating in the Information Environment*, avant une refonte doctrinale à paraître en 2020.

[39] *Air Marshal* E.J. Stringer CB CBE *Director General Joint Force Development and Defence Academy* : « This joint concept note explains why information advantage must be at the heart of how Defence operates if we are to enable credible military options and political utility, regain and maintain initiative, and achieve influence in a more complex and competitive world. » UK Ministry of Defence, « Information advantage », *Joint Concept Note* 2/18, p. iv.

[40] *Cyber und Informations Raum* (www.bundeswehr.de/de/organisation/cyber-und-informationsraum).

[41] La doctrine est en cours de rédaction, parution prévue fin 2020.

[42] Avec une production de qualité, à l'image du rapport paru en décembre 2019 au titre explicite : *Falling behind: How Social Media Companies are failing to combat Inauthentic Behaviour Online.*

[43] Initiative conjointe bien conduite par l'UE.

l'Allemagne et des pays d'Europe centrale pour une politique d'attribution ne va pas sans susciter parfois certaines différences d'analyses entre les pays membres. C'est le cas avec la France en particulier, notre pays faisant généralement le choix de ne pas attribuer publiquement ces attaques mais éventuellement d'en faire état directement aux pays concernés, l'attribution relevant d'une décision politique.

Les décisions prises par nos alliés traduisent l'importance qu'ils accordent tous à la prise en compte de cet espace de conflictualité. L'exemple américain est éclairant par la priorité donnée à ce domaine. C'est par exemple la décision de créer une 7e fonction interarmées, solution intéressante par son aspect transverse, mais également par l'intention de lier les opérations à l'information et non l'inverse. Ce sujet n'a pas été traité isolément mais comme conséquence d'une approche multidomaines. Les Américains ont d'abord pensé global au travers de leur concept *MDO*, notamment avant de décliner leurs efforts dans ce champ. Les changements d'ampleur amorcés par les Allemands semblent peu compatibles en première approche avec notre modèle, compte tenu de notre engagement permanent en opérations et des choix déjà faits pour ce qui a trait à l'Espace et au cyber. En revanche, la vision intégrée britannique est intéressante car elle apparaît comme une référence plus facilement transposable. Le domaine informationnel est à la fois clairement affiché comme priorité et décliné ensuite systématiquement à tous les niveaux dans une approche interministérielle qui mobilise les énergies et les moyens.

Des mesures prises et des pistes de réflexion pour faire face à cette menace en France

La comparaison avec nos principaux alliés pourrait nous faire apparaître en retrait dans l'espace informationnel. C'est partiellement vrai car un certain nombre de mesures ont été prises, tant dans le domaine civil que militaire, et parce que notre pays a fait le choix aussi, pour le moment, de s'appuyer sur des structures existantes. Ceci étant, une politique d'ensemble assortie d'une priorité de la part de l'État seraient néanmoins souhaitables pour faire face à cette menace qui va croissant.

De nombreuses initiatives mais sans stratégie d'ensemble

Sur le plan légal, deux lois font référence : la loi du 29 juillet 1881 sur la liberté de la presse [44] complétée par celle du 22 décembre 2018 relative à la lutte contre la manipulation de l'information [45]. Cette dernière, plus ciblée pour protéger les périodes préélectorales, a été instaurée pour éviter que ne se reproduisent des affaires comme celle des *Macron Leaks* en 2017. Du point de vue institutionnel, des cellules de veille sont actives au sein des différents organismes concernés et une coordination étendue a été mise en place sous l'égide du Secrétariat général de la défense et de la

[44] Loi du 29 juillet 1881 sur la liberté de la presse (www.legifrance.gouv.fr/).
[45] Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information (www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037847559&categorieLien=id).

sécurité nationale (SGDSN) pour ce qui concerne la menace exogène. Elles partagent ainsi les informations et organisent la réponse le cas échéant selon une logique extérieure-intérieure : ce qui vient de l'extérieur est une menace et à ce titre contré, et ce qui vient de l'intérieur est considéré comme une opinion dès lors qu'il ne s'agit pas de *Fake News*. Le ministère de l'Intérieur est très présent aussi avec la plateforme Pharos [46] qui intervient efficacement et rapidement sur les contenus illicites en ligne. Le Quai d'Orsay œuvre également, de son côté, en ayant désigné un ambassadeur pour le numérique en décembre 2018. Il traite tout d'abord avec les plateformes privées pour les amener à agir sur leurs contenus. Il construit ensuite, selon son expression, des « anticorps de la démocratie » : par l'intermédiaire de réseaux ouverts et collaboratifs regroupant des ONG et des citoyens engagés, il favorise les actions communes contre tout ce qui touche à la désinformation [47]. Ce type d'initiative participative a été très efficace en Suède par exemple, conduisant le site local de *Russia Today* à fermer faute d'audience. Enfin, les médias participent aussi activement à discriminer l'information qu'ils traitent. Ainsi ont-ils, pour les plus grands d'entre eux, mis en place des cellules appelées *fact-checking* pour authentifier leurs informations avant de les publier [48]. Cette liste des acteurs impliqués est bien sûr incomplète parmi toutes les initiatives existantes.

De leur côté, les armées prennent en compte cette menace comme précisé dans la *Revue stratégique* de 2017 [49] et le rapport annexé de la Loi de programmation militaire (LPM) 2019-2025 [50]. Elles mettent en œuvre en premier lieu une Stratégie militaire d'influence (SMI) pilotée depuis le bureau J9-OI (opérations d'information) du Centre de planification et de conduite des opérations (CPCO) et déclinée ensuite au niveau tactique en opérations d'information (InfoOps) en appui des forces engagées. Dans le même temps, les armées sont présentes dans le cyberespace où se joue une partie de cet affrontement *via* la Lutte informatique d'influence (LII). Cette dernière permet d'agir sur les informations, en augmentant leur visibilité ou en les supprimant par exemple, mais aussi de contrer des attaques informationnelles. Si l'aspect doctrinal et organisationnel n'a pas donné lieu à des évolutions comparables à celles de nos proches alliés, les moyens et capacités d'action ont été augmentés. Dans les faits, nous avons pu être contestés par des États sur des théâtres d'opérations moins visibles que le Sahel et notre réponse a été efficace [51]. Si ce type d'action sous le seuil d'emploi de la force survient à nouveau, cet exemple prouve notre savoir-faire et notre volonté dans ce domaine.

---

[46] Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action).

[47] Ambassadeur pour le numérique, « Des outils pour contrer la désinformation » (https://disinfo.quaidorsay.fr/fr).

[48] L'*AFP* emploie aujourd'hui par exemple 74 journalistes à plein temps dans cette mission et partage ses résultats en direct grâce à un site reconnu (https://factuel.afp.com/).

[49] Ministère des Armées, *Revue stratégique de défense et de sécurité nationale*, 2017, p. 46 (www.defense.gouv.fr/).

[50] « Réalités géostratégiques récentes rappelées par la *Revue stratégique*, cyberespace et champ de l'information constituent, de même, des espaces aussi vulnérables qu'accessibles à des actions malveillantes ou des agressions, qui exposent très directement les États, leur population, leurs services publics ou leurs entreprises à des dommages potentiels de grande ampleur. », p. 4 (www.defense.gouv.fr/).

[51] Entretien de l'auteur selon les règles de Chatham House.

Pour autant, la situation globale ne semble pas complètement satisfaisante dans la durée au regard des défis auxquels nous sommes confrontés. Culturellement tout d'abord, même si l'affaire des *Macron Leaks* a opéré une prise de conscience et levé une partie de notre inhibition, il subsiste encore des préventions importantes. Elles sont légitimes du point de vue démocratique et la question du contrôle des actions dès lors qu'elles augmenteraient en capacité et en périmètre serait à régler dans le même temps. Ces préventions nous conduisent aussi à être le plus souvent en réaction pour nous défendre. Cette posture pourrait nous épuiser et, par certains aspects, nous décrédibiliser dans le rôle « suspect » de celui qui se défend constamment. Il est enfin un sujet sensible entre tous – et une fragilité –, celui de la désinformation émise *via* un média en France et considérée aujourd'hui comme une opinion politique. À dessein, des médias d'origine étrangère par exemple relaient, nourrissent et amplifient cette désinformation sans en être forcément à l'origine, ce qui complique un peu plus ce débat. C'est une question d'une grande complexité et qui doit être traitée comme telle.

Une stratégie globale souhaitable, déclinée à tous les niveaux

Il ne s'agira pas ici de décréter que telle solution est à retenir plus que telle autre mais d'ouvrir des pistes de réflexion pour dépasser le constat. Tout d'abord, la logique européenne trouve tout son sens pour protéger les citoyens et notre modèle démocratique. La proposition du président de la République de créer une agence européenne de protection des démocraties pour préserver « les processus électoraux contre les cyberattaques et les manipulations [52] » s'inscrit dans cette démarche. C'est aussi par l'Europe que nous pourrons utilement peser sur les plateformes numériques privées. Avec l'exemple du Règlement général sur la protection des données (RGPD) [53], seule l'UE est en mesure de leur imposer une meilleure protection de nos données et une plus grande transparence dans leur usage, s'agissant notamment de la connaissance de leurs algorithmes.

Ensuite, ce qui a trait à l'organisation de l'État pourrait aussi évoluer. S'appuyer sur des structures existantes et des hommes en place ayant par ailleurs leurs propres missions ne semble pas viable dans la durée. Il convient de définir une stratégie interministérielle puis la décliner par des organisations et des moyens dédiés. La question se pose par exemple de laisser chaque ministère ou organisme faire sa propre veille et réagir, comme c'est le cas aujourd'hui. Cela peut avoir du sens si le sujet relève sans équivoque du ministère concerné [54]. C'est pourtant rarement le cas de manière claire car la veille, la réaction et l'action à proprement parler, nécessitent des moyens dédiés. Savoir s'il faut s'appuyer sur le SGDSN en augmentant ses capacités ou s'il est préférable de créer un organisme qui lui serait lié est un sujet à poser, notamment pour s'assurer que ces missions soient toutes prises en compte et coordonnées au bon niveau

[52] Macron Emmanuel, « Pour une renaissance européenne », 4 mars 2019 (www.elysee.fr/).
[53] Règlement UE 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (https://eur-lex.europa.eu/).
[54] L'intervention rapide du Minarm suite aux informations russes qu'un de ses avions aurait pu être abattu par une frégate française au large de la Syrie en 2018 a été ainsi très efficace (cf. *La Tribune*, 18 septembre 2018).

interministériel. Quoi qu'il en soit, cette stratégie ne doit pas être que défensive mais aussi imposer notre action de manière proactive et positive.

Dans le champ intérieur, une forme de haute autorité pourrait s'assurer du contrôle démocratique indispensable déjà évoqué. Celle-ci pourrait être à mi-chemin entre le Défenseur des droits et le *fact-checking*, en s'assurant de sa représentativité et de son contrôle comme celui qui s'exerce par l'intermédiaire des élus de la délégation parlementaire au renseignement. Un parquet spécialisé pourrait éventuellement compléter ce dispositif, en menant une politique de judiciarisation active des *Fake News*, à l'image de ce qui existe pour traquer la grande délinquance financière et économique, ou lutter contre le terrorisme. Cette question n'est certainement pas encore mûre mais le problème pose déjà un vrai défi à notre démocratie qui ne doit pas occulter ce sujet et prendre le temps d'y réfléchir.

Intégrer la Stratcom dans notre organisation et dès la conception des actions

Pour les armées, les mesures prises par nos alliés interpellent. Des transformations ont été conduites avec efficacité ces dernières années s'agissant de l'Espace et du cyber. En revanche, le champ informationnel n'a pas fait l'objet d'une même attention. La *StratCom* existe officiellement mais comme « concept à la maturité perfectible » [55]. Ainsi son périmètre serait à mieux définir et à élargir, son approche coordonnée mériterait d'être généralisée et pérennisée, et sa mise en œuvre, enfin, gagnerait à être liée dès l'origine aux actions – les modeler au besoin – plutôt que de les accompagner le plus souvent.

Pour prendre l'exemple des opérations, la responsabilité de la communication aujourd'hui appartient à la cellule éponyme de l'État-major des armées (EMA-COM) qui assure également la mission de porte-parole du Chef d'état-major des armées (Céma). Cette organisation se comprend par l'héritage centralisateur qui est le nôtre. Elle n'est en revanche pas compatible avec la mise en œuvre d'une *StratCom* déclinée à tous les échelons. Si les choix stratégiques doivent bien être effectués puis coordonnés à l'échelon central, la *StratCom* doit pouvoir aussi être déconcentrée pour être efficace. À titre d'exemple, l'opération multinationale *Inherent Resolve* (*OIR*) en Irak dispose de son porte-parole et anime ses propres réseaux sociaux. L'important ici est bien d'écrire et d'alimenter le narratif tous les jours, et dans la durée là où se déroule l'action principale, comme d'y contrer celui de l'adversaire. Cela suppose également que les chefs sur le terrain, non seulement disposent des moyens et de la subsidiarité nécessaires, mais aussi que soit admise une forme de « droit à l'erreur », rarement tolérée dès qu'il s'agit de communication. Il faut enfin que les chefs soient convaincus de la priorité à donner à la *StratCom* dans leur opération. Une évolution des mentalités devra donc aussi accompagner ce changement de priorité.

Après la concentration, le cloisonnement est également un frein à la mise en œuvre de la *StratCom*. Des améliorations sont en cours dans ce domaine aussi sans être

[55] DIA-3.10.0_STRATCOM, 2018, p. 6 [document classifié].

encore clairement formalisées. Seule une *StratCom* coordonnée peut rassembler utilement « l'équipe France ». Dans ce cadre-là, il serait souhaitable que l'ensemble des actions militaires produisant des effets – opérations, exercices à l'étranger, actions de soutien aux exportations, etc. – puissent être suivies et coordonnées de façon globale. C'est déjà le cas quand se regroupent de manière régulière à cette fin sur un théâtre d'opérations le commandant de la force, l'ambassadeur, l'attaché de défense ainsi que les autres acteurs civils et militaires concernés pour une mise en cohérence des actions et des messages.

La conduite de la *StratCom* pour les opérations revient pour partie aujourd'hui au bureau J9-OI du CPCO. Dès lors que ce domaine serait estimé prioritaire et bâti dès l'origine des actions, il semblerait nécessaire d'établir une « autorité *StratCom* » du grade de général [56] dont le positionnement serait à déterminer. Il devra rester en revanche au plus près des opérations et associer l'EMA-COM aux choix faits, pour que cette dernière puisse exercer un droit de regard en tant que « tête de chaîne » communication auprès du Céma.

Il est essentiel, à l'image de ce que font les Britanniques, que le décloisonnement du champ informationnel aille au-delà d'un cercle de spécialistes et qu'il devienne « l'affaire de tous » : dans la formation, dans les entraînements, en opérations, dans les casernes, cette menace doit être connue, intégrée et jouée à tous les niveaux. Pour préparer l'avenir, il serait par exemple souhaitable de faire évoluer la formation des officiers de manière à ce que les futures générations soient convaincues de ce besoin plus tôt et tout au long de leur carrière. En tactique, la recherche de la surprise est ainsi par excellence une action sur les perceptions. C'est un exemple possible pour la formation initiale, sachant qu'ils devront être capables par la suite de rechercher aussi des effets dans les champs immatériels.

Autre aspect d'une liste non exhaustive, une fois notre stratégie établie, nous devons aussi développer une action d'influence envers les instances internationales alliées sur ce domaine précis. Il s'agit de peser sur les réflexions et les décisions, en évitant par exemple de se voir imposer des attributions par ces mêmes organisations. Cette action ne peut exister sans commencer par honorer les postes concernés qui nous reviennent dans ces structures à l'Otan et à l'UE.

La *StratCom* est aussi une opportunité exceptionnelle pour une armée comme la nôtre soumise aux coûts toujours croissants de son matériel. Il ne s'agit pas de substituer le *Soft* au *Hard Power* mais bien de les faire agir de concert. Les actions dans le champ informationnel ont ainsi un faible coût par rapport aux résultats qui peuvent être obtenus. La guerre des Malouines en 1982 est un exemple emblématique du rôle qu'une *StratCom* efficace aurait pu jouer. Si les Argentins avaient ainsi été persuadés de la détermination des Britanniques à ne rien céder jusqu'à intervenir militairement si nécessaire, sans doute auraient-ils davantage réfléchi avant d'envahir ces îles [57].

---

[56] Pour lui donner la légitimité et la visibilité souhaitées en interministériel et en interalliés.

[57] « *Operation Corporate became necessary because deterrence failed* » comme le déclara l'amiral John Fieldhouse, commandant de la force interarmées britannique et futur *Chief of the Defence Staff* (CDS, équivalent du Chef d'état-major des armées), cité dans ROBERTS John, *Safeguarding the Nation: The Story of the Modern Royal Navy*, AMLIN, 2009.

Il est enfin un autre domaine qui devrait à son tour évoluer si la *StratCom* devenait une priorité. À l'heure où les résultats doivent être immédiats et transposables en indicateurs, ses effets se mesurent sur le temps long et pour partie en creux – nous en subissons en particulier les conséquences quand nous ne faisons rien (cf. guerre des Malouines). Des objectifs liés aux comportements peuvent être mesurables, moins les effets cognitifs. Il faut donc accepter que les efforts conduits dans ce domaine immatériel ne produisent pas nécessairement des effets à la fois tous immédiats et mesurables. C'est l'un des nombreux enseignements de la crise du Coronavirus que de voir certaines limites du modèle économique privé appliqué aux questions de défense [58].

⁂

« Si l'on veut avoir une influence sérieuse dans le monde, nous devons conserver suffisamment de forces militaires classiques relevant du *Hard Power*, pour pouvoir engager des actions de *Soft Power*. L'un ne va pas sans l'autre. Le pouvoir politique doit bien en prendre conscience [59] ». Cette réflexion du général Desportes semble d'évidence. Il est illusoire de penser que le *Soft Power* sera efficace sans l'assise de la puissance. Toutefois à l'heure où l'approche directe est de plus en plus coûteuse financièrement, il est indéniable qu'un investissement adapté dans le champ informationnel aurait une forte rentabilité en plus de répondre à un besoin de protection. Les Britanniques, dans le cadre des travaux préparatoires de l'*Integrated Review* [60] lancés en 2020, ont clairement la tentation de céder aux sirènes de la seule rentabilité en se recentrant sur leur *Soft Power* [61] derrière leur slogan *Global Britain* et dans la continuité du mouvement qui a présidé au *Brexit*.

Le champ informationnel comme nouvel espace de conflictualité à l'ère numérique reste un enjeu majeur inédit par le niveau de menace croissant tous azimuts qu'il fait peser sur nous. Nos opérations militaires et leur réussite lui sont intimement liées. Plus fondamentalement, il représente un vrai défi pour notre modèle démocratique. Ce constat lucide de la situation actuelle, de la menace présente et potentielle à venir, et du cadre dans lequel nous évoluons doit nous amener à réfléchir d'abord aux stratégies que nous souhaitons conduire pour y répondre le plus efficacement – civile et militaire, par domaine ou globale, dans le cadre actuel ou à redéfinir – et ensuite aux organisations et ressources à y consacrer. Nous disposons, d'ores et déjà, de vrais atouts qui se traduisent en autant d'initiatives à tous les niveaux, atouts parmi lesquels la prise de conscience au sommet de l'État n'est pas le moindre. La prévention dont nous avons hérité doit rester une sorte de garde-fou par rapport à la sensibilité politique de ce sujet.

---

[58] « Cela correspond, à mon sens, à un mode de gestion des entreprises qui a contaminé la sphère publique alors que leurs finalités sont fondamentalement différentes. La raison d'être d'un État, c'est avant tout d'assurer la sécurité physique de ses ressortissants. En Europe, on a tenu les notions de plan et de planification pour obsolètes au profit d'outils de gestion à horizon trimestriel. », Gomart Thomas, *op. cit.*

[59] Desportes Vincent, *op. cit.*

[60] Revue stratégique globale mêlant politique internationale et capacités militaires.

[61] Roberts Peter, *The Integrated Review: Rebuilding the UK's Hard Power*, RUSI Newsbrief, 21 février 2020 (https://rusi.org/publication/rusi-newsbrief/integrated-review-rebuilding-uk%E2%80%99s-hard-power).

Elle ne doit pas en revanche être un frein par désintérêt ou inhibition. C'est là que doit porter notre premier effort.

Une caractéristique du champ informationnel reste l'inégalité par nature du combat qui y est mené. La « charge de la preuve » y est inversée en quelque sorte et c'est bien à la vérité de s'imposer face au mensonge et non l'inverse. Érasme ne dit pas autre chose. Cette situation serait censée donner un avantage définitif aux régimes autoritaires, nos compétiteurs stratégiques. De manière contre intuitive pourtant, il faut garder à l'esprit que les démocraties ne sont pas totalement démunies [62] pour faire face à ces défis : « les régimes démocratiques et libéraux sont, à terme, plus efficaces. Ils facilitent l'innovation, ils permettent le consensus, ils réduisent le risque de dérive autoritaire, avec ce que cela engendre de corruption et donc d'inefficacité sociale ; ils valorisent le mérite. Au demeurant, les instruments utilisés par les régimes autoritaires pour nous déstabiliser n'ont pu être développés que dans des sociétés ouvertes » [63]. Le combat ne fait que commencer et si nous ne sommes pas complètement démunis en effet, la fragilité qui sera la nôtre au sortir de la crise du Covid-19 devrait nous inciter plus que jamais à nous donner sans délai les moyens de nous protéger, de nous défendre et de combattre dans le champ informationnel pour préserver notre modèle démocratique.

Éléments de bibliographie

« Avion russe abattu : malgré la faute de l'armée syrienne, la Russie menace Israël de représailles », *La Tribune*, 18 septembre 2018 (www.latribune.fr/).

AFP, « À Versailles, Macron a parlé cash à Poutine sur la Syrie, les Droits de l'Homme ou les médias russes », *La Croix*, 30 mai 2017 (www.la-croix.com/).

AFP, *Le* fact-checking *par l'*AFP (https://factuel.afp.com/).

Ambassadeur pour le numérique, « Des outils pour contrer la désinformation » (https://disinfo.quaidorsay.fr/fr).

Amer Karim et Noujaim Jehane, *The Great Hack : l'affaire Cambridge Analytica*, Netflix, 2019, 1h54.

Bernard Michel, *Hiver 1814, campagne de France*, Perrin, 2019, 240 pages.

BuzzFeedVideo, « You Won't Believe What Obama Says in This Video! », *Youtube*, 17 avril 2018 (https://m.youtube.com/watch?v=cQ54GDm1eL0).

Centre d'excellence pour la communication stratégique de l'Otan, *Falling Behind: How Social Media Companies are failing to combat Inauthentic Behaviour Online*, décembre 2019 (www.stratcomcoe.org/).

Desportes Vincent, « Opérations extérieures et opérations d'influence », *Communication & Influence*, n° 40, janvier 2013 (www.comes-communication.com/).

DIA-3.10.0_STRATCOM, 2018 [document classifié].

Duneau Clémence, « Facebook : comment le discours de Mark Zuckerberg a changé en quatorze ans », *Le Monde*, 11 avril 2018 (www.lemonde.fr/).

Fourquet Jérôme, *L'Archipel français*, Seuil, 2019, 384 pages.

(62) Les Russes prêtent ainsi aux Américains la responsabilité des « révolutions de couleur » (cf. « Vers de nouvelles révolutions de couleur ? Soros verse 18 mds USD à Open Society », *Sputnik*, 18 octobre 2017 ; https://fr.sputniknews.com/) alors que les démocraties ne peuvent user des mêmes moyens que ceux des États autoritaires.

(63) Le Drian Jean-Yves, *op. cit*.

GUILLUY Christophe, *La France périphérique : Comment on a sacrifié les classes populaires*, Flammarion, 2014, 185 pages.

JEANGÈNE VILMER Jean-Baptiste, ESCORCIA Alexandre, GUILLAUME Marine, HERRERA Janaina, *Les Manipulations de l'information*, Caps-Irsem (Centre d'analyse, de prévision et de stratégie-Institut de recherche stratégique de l'École militaire), août 2018, 210 pages (www.diplomatie.gouv.fr/).

JEANGÈNE VILMER Jean-Baptiste, *The « Macron Leaks » Operation : A post-Mortem*, Atlantic Council-Irsem, juin 2019 (www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf).

LE DRIAN Jean-Yves, « Discours de clôture de la conférence internationale "Sociétés civiles, médias et pouvoirs publics : les démocraties face aux manipulations de l'information" », Paris, 4 avril 2018 (www.diplomatie.gouv.fr/).

LEVASSEUR Guillaume, *Mise en perspective stratégique des techniques numériques émergentes de falsification des informations sur* Internet (thèse professionnelle de master spécialisé), Telecom ParisTech, novembre 2018.

LIDDELL HART Basil H., *Stratégie*, Perrin, 2017 (édition originale 1954).

MACRON Emmanuel, « Pour une renaissance européenne », 4 mars 2019 (www.elysee.fr/).

NYE Joseph S., *Soft Power, The Means to Success in World Politics,* Public Affairs, 2004, 208 pages.

PARLY Florence, « Discours de la ministre des Armées de clôture de l'université d'été de la Défense », Avord, 13 septembre 2019 (www.vie-publique.fr/discours/270451-florence-parly-13092019-politique-de-defense).

PLANCHAIS Jean, « À la rubrique défense du journal *Le Monde* 1945-1965 », *in* FORCADE Olivier, Duhamel Éric, VIAL Philippe (dir.), *Militaires en République 1870-1962*, Publications de La Sorbonne, 1999, p. 536-537.

Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action).

POMERLEAU Mark, « Two years in, how has a new strategy changed cyber operations? », *FifthDomain*, 11 novembre 2019 (www.fifthdomain.com/).

Rapport annexé de la loi de programmation militaire (LPM) 2019-2025 (www.defense.gouv.fr/).

ROBERTS John, *Safeguarding the Nation: The Story of the Modern Royal Navy*, AMLIN, 2009, 320 pages.

ROBERTS Peter, *The Integrated Review: Rebuilding the UK's Hard Power*, RUSI Newsbrief, 21 février 2020 (https://rusi.org/publication/rusi-newsbrief/integrated-review-rebuilding-uk%E2%80%99s-hard-power).

SEMO Marc, « Thomas GOMART : "La crise due au coronavirus est la première d'un monde *post*-américain" », *Le Monde*, 8 avril 2020.

TENENBAUM Élie, *Partisans et centurions, une histoire de la guerre irrégulière au XX^e siècle*, Perrin, 2018, 528 pages.

The Washington Post, « Pelosi videos manipulated to make her appear drunk are being shared on social media », 23 mai 2019 (www.youtube.com/watch?v=sDOo5nDJwgA).

UNITED STATES ARMY TRAINING AND DOCTRINE (TRADOC), *The US Army in Multi-Domain Operations 2028*, 6 décembre 2018 (www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf).

US CYBER COMMAND, *Achieve and Maintain Cyberespace Superiority, Command Vision for US Cyber Command*, 2018, 12 pages (https://nsarchive.gwu.edu/).

US DEPARTMENT OF DEFENSE, *Joint Concept for Operating in the Information Environment (JCOIE)*, 25 juillet 2018 (www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830#).

VARGAS José Antonio, « The face of Facebook », *The New Yorker*, 13 septembre 2010 (www.newyorker.com/).

WYLIE Christophe, *Mindfuck : Le complot Cambridge Analytica pour s'emparer de nos cerveaux,* Grasset, 2020, 512 pages.