L'INFLUENCE MILITAIRE DANS LA NOUVELLE PENSÉE STRATÉGIQUE FRANÇAISE

Nicolas Zubinski

Comité d'études de Défense Nationale | « Revue Défense Nationale »

2021/2 N° 837 | pages 75 à 83

ISSN 2105-7508

Article disponible en ligne à l'adresse :

https://www.cairn.info/revue-defense-nationale-2021-2-page-75.htm

L'influence militaire dans la nouvelle pensée stratégique française

Nicolas Zubinski | Expert en intelligence économique et communication stratégique ; rédacteur « Sécurité nationale » du site infoguerre.fr, Centre de réflexion sur la guerre économique, École de Guerre Économique.

Peu connue du grand public, l'influence militaire rassemble les capacités militaires dites non-cinétiques d'action sur les perceptions et de modification des comportements. La doctrine militaire française y intègre classiquement les opérations psychologiques [1], les opérations d'informations [2], les actions civilo-militaires [3] et une déclinaison dans l'environnement informatique *via* la lutte informatique d'influence (LII) qui devrait prochainement évoluer en « lutte informationnelle dans le cyberespace » (LIC) [4].

Or, les conflits sont marqués par une augmentation des affrontements dans le champ cognitivo-informationnel soutenus par la montée en puissance de la dimension numérique sous toutes ses formes (réseaux sociaux, vidéos, *tweets*, etc.). Une réflexion de fond sur un potentiel retour à l'emploi des capacités militaires d'influence était nécessaire. Lors de son audition à l'Assemblée nationale sur le projet de loi de finances pour 2020, le général Thierry Burkhard, chef d'état-major de l'Armée de terre (Cemat), marquait sa volonté d'« investir de nouveaux champs : cyber, déception, résistance à la désinformation ou encore meilleure prise en compte de l'influence » [5]. L'Armée de terre s'y prépare activement, que cela soit par l'infovalorisation des systèmes d'armes ou par la simulation d'actions d'influence sur les réseaux sociaux [6].

C'est ainsi un nouveau type de conflictualité qui est apparu. Les sociétés sont soumises, par une guerre de l'information, à un stress permanent de déstabilisation, voire de remodélisation, dans le but de modifier les comportements à l'échelle géostratégique. Et pourtant l'information projetée n'y est qu'un vecteur de coordination des effets d'influence dans le jeu des gouvernements, dans la concurrence et la rivalité des groupes sociaux. C'est dire à quel point l'analyse systémique de l'environnement civil des opérations permet d'amplifier l'impact des approches indirectes.

Les nouvelles guerres délinéarisées, indirectes et *post*-hybrides du XXIe siècle

De nouvelles formes de continuation de la politique par la guerre

Les stratégies d'influence entre États sont historiquement l'expression d'une continuation de la conflictualité durant les périodes de paix. Les effecteurs mobilisés étaient à dominante civile (représentations diplomatiques, entreprises, fondations, organisations non gouvernementales, associations, etc.), et ceux de nature militaire contribuaient essentiellement par le renseignement. Mais l'avènement des conflits hybrides et non-linéaires [7] a fait entrer la fonction militaire dans une sphère jusqu'alors essentiellement civile. La mutation est double : d'une culture du renseignement tactique (hérité de Clausewitz) à une culture de l'influence et des intelligences (davantage portée par Sun Tzu). Les forces armées se trouvent confrontées au nouveau paradigme polémologique [8] des conflits du XXIe siècle.

L'avènement d'une conflictualité post-*hybride et indirecte*

Les doctrines chinoises (Liang-Xiangsui) [9] et russes (Primakov-Guérassimov) [10] d'hybridation et de délinéarisation des conflits ont innové en repensant l'articulation des effecteurs militaires dans leur stratégie de puissance. Les capacités militaires d'influence sont mises au service de buts de guerre « hors limites », à dominante civile. Cela revient à inverser la logique d'hybridation des conflits telle que nous la connaissons. Il ne s'agit plus de recourir, pour les forces armées, à des moyens civils dans le but d'atteindre des objectifs militaires, mais au contraire d'utiliser des capacités militaires, notamment d'influence et de renseignement élargi, afin d'atteindre des objectifs de puissance civile.

Le XXIe siècle voit considérablement augmenter l'utilisation des capacités militaires dans des guerres auxquelles les armées n'étaient pas préparées : qu'elles soient économiques [11], politiques [12] et sociétales [13]. La guerre ne se déclare plus. Ce basculement marque l'entrée dans une ère *post*-hybride procédant d'un renversement des logiques d'emplois entre les effecteurs cinétiques et non cinétiques à des fins d'influence. Le recours à des approches indirectes se généralise, de même que les finalités politiques d'emploi de capacités militaires se civilisent. En somme, de nouvelles façons et raisons de conduire la guerre ont émergé et force est de constater que ces nouveaux conflits indirects ont pour dénominateur commun la guerre de l'information.

La militarisation du cyberespace et la manipulation des opinions publiques

La militarisation du cyberespace joue d'ailleurs un rôle essentiel dans cette évolution. L'utilisation du vecteur informatique dans le champ cognitif marque un tournant dans les stratégies d'emploi des effecteurs d'influence [14]. Les ingérences

russes de 2016 dans la campagne présidentielle américaine et dans le vote de sortie de l'Union européenne du Royaume-Uni (*Brexit*) mettent en lumière la vulnérabilité des sociétés occidentales aux effecteurs militaires d'influence. Les modes opératoires sont désormais bien connus, et la Direction nationale du renseignement américain (DNI) conclut dès 2017 que « la campagne d'influence de Moscou a suivi une stratégie de messagerie russe qui allie des opérations secrètes – telles que la cyberactivité – aux efforts manifestes des agences gouvernementales russes, des médias financés par l'État, des intermédiaires tiers et des utilisateurs rémunérés de médias sociaux ou *trolls* » [15], rendant d'autant plus difficile l'« attribution » de ces actions.

Passant de l'attaque contre des systèmes informatiques (depuis 2007, Estonie) à de l'attaque informationnelle (telle l'ingérence russe, 2016), la variété des menaces informatiques aura marqué une escalade dans la lutte pour l'influence. En outre, de plus en plus d'États l'ont intégré dans leur stratégie d'influence. Le DNI a ainsi constaté que si la Russie était coutumière des manipulations d'opinions publiques, l'Iran et la Chine ont multiplié les tentatives d'interférence sur l'élection présidentielle américaine de 2020 [16].

Vers une nouvelle guerre froide aux degrés d'intensité variable ?

Le nouveau concept britannique d'emploi des forces constate la généralisation de l'emploi des capacités militaires d'influence dans des affrontements indirects de puissance [17], analyse partagée par la RAND Corporation [18]. Néanmoins, le général Thierry Burkhard soulignait que « les conflits se durcissent et nos compétiteurs sont très habiles ! De plus en plus de pays agissent juste sous le seuil du conflit ouvert avec des actions non revendiquées : attaques cyber, opérations d'influence et de manipulation de l'opinion publique, des domaines où l'attribution de l'attaque est difficile. Ils n'hésitent plus à déployer leurs forces, à tester parfois brutalement, à intimider » [19]. Et de considérer que les prochains conflits seront de haute intensité, c'est-à-dire faisant face à des adversaires « capables de contester notre supériorité dans l'ensemble des milieux » [20]. Bien que les constats britannique et français sur l'évolution de l'intensité s'opposent, ces deux visions stratégiques soulignent en définitive que les capacités d'influence prospèrent tant dans une stratégie indirecte et non-cinétique, qu'au cœur de théâtres plus classiquement cinétiques.

À cet égard, la position française offre l'avantage d'adapter les forces conventionnelles aux effets dans les champs immatériels, d'où l'effort technologique croissant sur l'infovalorisation et la dimension spatiale (Geo-Int), ainsi que l'intégration de la guerre de l'information jusque dans les manœuvres de l'Armée de terre. Les évolutions décrites n'excluent évidemment pas la persistance de conflits plus classiquement cinétiques et aux moyens conventionnels qu'ils emploient. Les priorités ne pouvant pas se multiplier, un choix d'orientation stratégique s'impose.

Or, face à des ingérences sur le territoire informationnel national en Grande-Bretagne et aux États-Unis, ces deux États ont choisi d'investir dans des capacités d'influence psycho-informationnelles de basse intensité.

Le degré d'intensité semblerait en définitive varier selon le territoire sur lequel il s'exprime. Un affrontement de haute intensité entre grandes puissances sur leurs territoires nationaux semble peu probable. À cet égard, l'analyse anglo-saxonne des menaces tend à considérer que les affrontements porteront, sur ce type de théâtres, essentiellement dans le champ immatériel pour déstabiliser un État sans entrer dans un conflit armé. Il est donc plus simple de frapper le territoire national sans recourir à un conflit armé. Toutefois, s'agissant d'un affrontement sur des territoires étrangers, par *proxy*, l'analyse française exprime clairement le risque croissant d'escalade de l'intensité. Ainsi, la multipolarisation du monde contribue à la fois à durcir les opérations d'influence dans le champ immatériel et à « cinétiser » les confits dans les sphères d'influence des grandes puissances. Dans ces deux types de conflits, les capacités militaires sont nécessaires pour rendre inopérantes les opérations de déstabilisation. Dans ce cas, l'analyse britannique des nouvelles menaces pourrait surtout être l'annonce d'un désengagement des forces conventionnelles britanniques sur les théâtres d'opérations compensé par un appui aux alliés otaniens centré sur les capacités d'influence.

Préparer l'armée aux nouvelles guerres de l'information

La divergence franco-britannique porte également sur le mandat accordé aux militaires. L'acception anglo-saxonne du concept de sécurité nationale permet une plus grande facilité de coordination des effecteurs militaires et civils contre une ingérence étrangère. *A fortiori*, cela se vérifie lorsque l'ingérence est de nature cyber, et entre dans le champ psycho-informationnel. Alors que dans l'organisation dichotomique française renvoyant défense et sécurité nationale, la légitimité du ministère des Armées (MinArm) à s'intégrer dans une contre-ingérence informationnelle ne va pas de soi, sans pour autant justifier celle du ministère de l'Intérieur (MinInt). Le MinArm est, à l'heure actuelle, le mieux outillé pour défendre l'environnement informationnel dans le cyberespace français (lignes budgétaires, volume de ressources humaines dédiées, investissements matériels, architecture polyvalente, recherche stratégique). Malgré cela, certains observateurs civils s'interrogent sur la capacité du MinArm à concevoir et à orchestrer une guerre de l'information [21]. Il faut ici distinguer deux enjeux. Le premier réside dans la construction d'une capacité opérationnelle transministérielle de mise en œuvre. Le second relève de la stratégie d'emploi des effecteurs et des règles d'engagement des actions psycho-informationnelles. À ce titre, la doctrine interarmées française de stratégie militaire d'influence (SMI) et d'opérations d'information (Info-OPS) mériterait une refondation pour rendre les capacités d'actions dans le champ immatériel extérieur plus offensives, mais également de faciliter le soutien des forces de l'ordre dans la défense du champ immatériel intérieur.

L'importance grandissante de l'environnement civil des opérations

En civilisant les objectifs de guerre, la nouvelle conflictualité du XXIe siècle a également augmenté l'importance des activités civiles dans l'environnement humain des opérations.

Guerre de l'information et opérations de déstabilisation politiques et sociétales

Les tentatives de manipulation des opinions publiques et ingérences électorales par des vecteurs militaires d'influence ont placé les autorités civiles au cœur du centre de gravité des États. Bien entendu, la déstabilisation d'États par l'environnement civil n'est pas une innovation. En revanche, l'amélioration continue des capacités d'analyses systémiques, du ciblage et des mesures d'impact a considérablement augmenté l'efficience de ce type d'actions. Les opérations militaires dans le champ informationnel de ces dernières années ont impacté l'environnement civil de deux manières : l'une vise la remodélisation de l'échiquier sociétal ; l'autre, la déstabilisation du processus décisionnel d'un État. Ainsi, la conflictualité informationnelle n'est plus l'apanage de la guerre « politique », mais a fait émerger une guerre « sociétale ».

La guerre politique a pour but d'influencer le processus décisionnel d'un État afin d'obtenir une modification de sa politique conforme aux intérêts de l'attaquant. Les exemples d'ingérences russes, iraniens et chinois dans les processus électoraux procèdent de ce nouveau type de conflictualité.

Alors que la guerre sociétale a pour but d'altérer le système de valeurs et de croyances d'une société ou d'un État, c'est-à-dire le référentiel cognitif commun à l'auditoire national, afin de déstabiliser la cible de l'attaque par une remodélisation de son environnement. À titre illustratif, la stratégie radicalisation islamiste en cours en France depuis les années 1990 [22] procède de ce mode opératoire ; de même, la crise Covid-19 serait également le terreau d'actions de cyber-déstabilisation répondant à des logiques de guerre sociétale [23].

Approche sociétale et technique de remodélisation environnementale

Le développement des actions dans l'environnement civil des opérations ne se limite pas à une intensification de la guerre de l'information. Il s'agit également de l'expression de nouveaux modes d'action ouverts par des capacités d'analyse renforcées. En affinant la compréhension des interactions entre environnements (notamment psycho-informationnel et socio-économique), des modes opératoires plus difficilement perceptibles sont apparus. Les actions systémiques dans l'environnement civil participent d'une évolution des approches indirectes et permettent d'ouvrir le champ à de nouvelles capacités de modification comportementale par modelage des champs matériels et immatériels de l'environnement civil. Ainsi, comme le

décrit Raphaël Chauvancy, « cette approche signifie que la cible n'est plus simplement l'ennemi, mais l'environnement. Seule une vision à moyen et long termes permettra de le modeler favorablement en reprenant le contrôle du rythme stratégique » [24].

En cherchant à modifier le référentiel sociétal, les actions d'influence ne se limitent plus à modifier la perception des auditoires civils cibles, mais vont jusqu'à la remodélisation de leur environnement. Ce n'est en somme qu'une application militaire des techniques de *market shaping* usuelles dans les entreprises disposant de capacités spécialisées en influence et analyse de marché. S'ajoute à l'amplification de la guerre de l'information, une menace plus profonde de remodélisation des sociétés qui offre à l'adversaire l'avantage d'avancer sous le seuil de conflictualité armée, donc de passer inaperçu. L'approche indirecte environnementale est historiquement pratiquée par les États-Unis dans leur stratégie de guerre économique et de *soft power* visant la création d'une dépendance économique durable. Elle l'est également par les promoteurs de l'islam politique dans leur stratégie de radicalisation des sociétés musulmanes et de conquête des sociétés occidentales [25].

L'approche environnementale, une opportunité pour les actions de stabilisation

Les techniques de remodélisation environnementale permettent par ailleurs d'amplifier les actions de stabilisation des théâtres d'opérations. En effet, si les actions de remodélisation sociétale étaient historiquement mises en œuvre sur une ou plusieurs décennies (exemple de l'Allemagne et du Japon *post*-1945 ; ou de l'Irak *post*-2004 dans la logique *nation building*), la numérisation des sociétés a amplifié l'impact de ce mode opératoire, et accéléré les processus de modification comportementale. La généralisation de l'approche environnementale dans la planification stratégique des opérations peut contribuer ainsi à limiter les risques d'endiguement des conflits, et à faciliter les missions de promotion des intérêts nationaux.

L'impact des nouvelles stratégies d'influence militaire sur la coopération ministérielle du MinArm

Le développement des capacités militaires d'influence pourrait utilement appuyer deux autres acteurs ministériels : d'une part, le ministère de l'Europe et des Affaires étrangères (MEAE), dans une perspective d'amélioration opérationnelle de l'approche globale ; d'autre part, le MinInt, dans une perspective de renforcement de sa fonction de contre-ingérence. La portée opérationnelle de ces capacités pourrait être renforcée par une coopération transministérielle structurée de niveau stratégique.

Une opportunité de renforcement de l'approche globale sur les théâtres extérieurs

S'agissant du MEAE, la coordination de la communication stratégique avec des actions civilo-militaires et des actions civiles de stabilisation permettrait une meilleure modélisation d'un environnement sociétal stable et prospère. L'action dans la sphère sociétale permet de subjectiver les effets neuropsychologiques dans la vie quotidienne des individus, et ainsi de renforcer les actions dans le champ immatériel par des projets concrets et perceptibles.

Cela suppose de renforcer l'intégration de l'effecteur privilégié du MEAE, c'est-à-dire le Centre de crise et de soutien (CDCS), dans le processus de planification des opérations. Et ainsi, de créer une fonction de pilotage stratégique permettant le déploiement d'un processus de modélisation sociétale facilitant la stabilisation d'un théâtre.

Qui plus est, en augmentant les matrices d'effets et d'impacts des armées par la prise en compte des objectifs civils de stabilisation, le suivi pluriannualisé de la stabilisation serait renforcé. Là où l'approche environnementale indirecte avait permis aux agents déstabilisateurs de renforcer leur influence, il est possible de retourner ce mode opératoire pour endiguer leur progression, de forger une résilience sociétale et de faciliter l'émergence des conditions d'une paix durable.

Intégrer l'influence et la contre-ingérence dans de la coordination interministérielle du renseignement

S'agissant du MinInt, l'amplification des ingérences extérieures dans les champs immatériels français a été constatée par les services spécialisés du MinArm. La *Revue stratégique de défense et de sécurité nationale* de 2017 avait déjà souligné « la perméabilité des sociétés européennes aux influences extérieures » ainsi que l'« influence accrue des acteurs non étatiques (organisations terroristes ou criminelles, grandes multinationales, diasporas) » [26]. Il importe donc de construire des capacités de défense de nos auditoires nationaux contre des actions d'influence étrangère. Or, cette stratégie de défense nécessite l'emploi combiné de capteurs et d'effecteurs issus de ministères différents, à savoir le MinInt et le MinArm.

Pour autant, il n'existe pas en France de doctrine interministérielle de guerre de l'information permettant à la contre-ingérence (relevant de la DGSI du MinInt) de s'articuler avec les effecteurs militaires d'influence (relevant au sein du MinArm du Comcyber, du CIAE, du COS et de la DGSE). Et cette séparation ministérielle est aujourd'hui en inadéquation avec cette menace, qu'elle soit intérieure ou extérieure. L'emploi des capacités militaires d'influence mériterait d'être intégré dans un concept élargi de sécurité nationale afin de concevoir une doctrine transministérielle de guerre de l'information et de contre-influence.

Mais ce concept n'est pas bien perçu au plus haut niveau de l'État ou par les auteurs de la loi sur le renseignement, préférant une approche sectorielle de la sécurité ou des intérêts nationaux relevant de portefeuilles ministériels différents (défense, sécurité intérieure, sécurité économique) [27] sans véritable coordination. Les opérations étrangères d'influence ne dissocient pas les actions selon les vecteurs ou les échiquiers. Bien au contraire, l'ère des approches indirectes systémiques vise justement à agir de manière simultanée et combinée. Dès lors, l'approche organique visant à dissocier renseignement et influence. Penser la sécurité économique en dehors de la sécurité nationale, en omettant la militarisation croissante des actions d'influence étrangère dans les échiquiers économiques et sociétaux, révèle notre faiblesse idéologique.

L'heure n'est pas à la spécialisation des approches sécuritaires, mais à la coopération transministérielle pour faciliter l'émergence de réponses efficaces, c'est-à-dire systémiques. Il faut à terme concevoir des protocoles d'emploi des capacités militaires d'influence par les ministères civils pour organiser la défense opérationnelle de l'environnement informationnel français. En plus d'améliorer les capacités d'analyses de la menace, cette approche résolument pragmatique permet de pallier les contraintes budgétaires. Plutôt que d'atomiser les capacités par portefeuille ministériel, l'effort doit porter sur la facilitation des mises à disposition transministérielles et donc sur la mise en place d'un organe de pilotage unitaire, au niveau stratégique donc présidentiel. La transministérialité apparaît à la fois comme une réponse de bonne gestion administrative et financière, mais aussi comme un gisement d'optimisation de la réponse étatique aux ingérences extérieures, comme le fut la CNR *post*-2017 (contre le terrorisme). Ainsi, la nouvelle conflictualité du XXI^{e} siècle force les acteurs publics de la défense et ceux de la sûreté intérieure à plus de syncrétisme.

ÉLÉMENTS DE BIBLIOGRAPHIE

[1] Centre interarmées de concepts, de doctrines et d'expérimentation (CICDE) : *Doctrine interarmées* n° DIA-3.10.1(A)_PSYOPS.

[2] CICDE : *Doctrine interarmées* n° DIA-3.10(A)_SMI-INFO-OPS

[3] CICDE : *Doctrine interarmées* n° DIA-3.19_CIMIC

[4] Laurent Lagneau : « Les forces françaises vont se doter d'une doctrine de « lutte informationnelle dans le cyber-espace » », *Zone militaire opex360.com*, 14 juillet 2020 (www.opex360.com).

[5] Audition du général Thierry Burkhard (Cemat) sur le projet de loi de finances pour 2020, Assemblée nationale, Commission de la défense nationale et des forces armées, 17 juin 2020 (www.assemblee-nationale.fr).

[6] Nicolas Barotte : « L'Armée de terre s'entraîne à la guerre de l'information », *Le Figaro*, 8 octobre 2020 (www.lefigaro.fr).

[7] Dr Can Kasapoglu : « Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control », OTAN-NATO Defense College, Rome, novembre 2015 (www.ndc.nato.int). Tad A. Schnaufer II : « Redefining Hybrid Warfare: Russia's Non-linear War against the West », *Journal of Strategic Security*, vol. 10, n° 1 art. 3, 2017 (www.scholarcommons.usf.edu).

[8] La polémologie se définit comme l'« étude scientifique de la guerre considérée comme phénomène psychologique et social », Centre national de ressources textuelles et lexicales (CNRTL). Pour une synthèse de l'approche polémologique, voir l'article de Frédéric Coste : « Bouthoul et la polémologie : l'étude des causes profondes de la guerre », *Les Champs de Mars*, n° 12, 2002/2 (www.cairn-int.info).

[9] Colonels Qiao Liang et Wang Xiangsui : « La guerre hors limites », mars 2006 (version française poche, mais 1999 pour l'édition américaine de la CIA), Payot, Rivages poche, Petite bibliothèque.

[10] Général et chef d'état-major Valeri Guérassimov (ministère de la Défense de la Fédération de Russie) : « Value of science in forecast », *Military-Industrial Kurier,* 27 février 2017 (www.vpk-news.ru).

[11] Henri Martre (dir.), avec Philippe Clerc, Christian Harbulot, Philippe Baumard, Bernard Fleury, Didier Violle : *Intelligence économique et stratégie d'entreprise*, La Documentation française, février 1994 (www.entreprises.gouv.fr).

[12] Pr. Mark Galeotti : *Russian Political War: Moving Beyond the Hybrid*, Routledge: Taylor & Francis Group, 2019.

[13] Nicolas Zubinski : « Le concept de guerre sociétale : mutation des *political & information warfares* », 20 mai 2020, Centre de réflexion sur la guerre économique, École de Guerre Économique (www.infoguerre.fr).

[14] Brad Boyd et Herbert Lin : « Affecting the Cognitive Dimension of the Information Environment through Cyber-Enabled Information Operations », *Journal of Information Warfare* (*JIW*), 2019 (www.jinfowar.com).

[15] Office of the Director of National Intelligence, Intelligence Community Assessment : « Assessing Russian Activities an Intentions in Recent US Elections », janvier 2017, page ii (www.dni.gov).

[16] Office of the Director of National Intelligence : « Statement by NCSC Director William Evanina: Election Threat Update for the American Public », 7 août 2020 (www.dni.gov).

[17] UK Ministry of Defence (MOD) : « The Integrated operating concept 2025 », Ministry of Defence - MOD, 30 septembre 2020 (assets.publishing.service.gov.uk).

[18] Raphael S. Cohen, Nathan Chandler, Shira Efron, Bryan Frederick, Eugeniu Han, Kurt Klein, Forrest E. Morgan, Ashley L. Rhoades, Howard J. Shatz, Yuliya Shokh : « The Future of Warfare in 2030: Project Overview and Conclusions », RAND Corporation, 2020 (www.rand.org).

[19] Audition du général Thierry Burkhard portant sur la nouvelle vision stratégique de l'Armée de terre, Assemblée nationale, Commission de la défense nationale et des forces armées, 17 juin 2020 (www.assemblee-nationale.fr).

[20] Général Thierry Burkhard, propos recueillis par Jean-Dominique Merchet dans « L'Armée de terre se prépare au retour de la guerre de haute intensité », *L'Opinion*, 11 mars 2020, avec la collaboration de l'Institut français des relations internationales - Ifri (www.lopinion.fr).

[21] Christian Harbulot : « L'armée française a-t-elle les moyens de mener une guerre de l'information ? », 9 octobre 2020, Centre de réflexion sur la guerre économique, École de Guerre Économique (www.infoguerre.fr)

[22] Éric Delbecque : *Les Silencieux - Ne nous trompons pas, les salafistes menacent la république*, Plon, 2020.

[23] Franck Decloquement : « Covid-19 : comment les pirates informatiques exploitent férocement la déstabilisation des États, des entreprises… et des particuliers », *Atlantico*, 21 mai 2019 (www.atlantico.fr).

[24] Raphaël Chauvancy : « Le nouveau concept d'emploi des forces britanniques, une révolution stratégique », 6 octobre 2020, revue *Conflits* (www.revueconflits.com).

[25] Bernard Rougier (dir.) : *Les Territoires conquis de l'islamisme*, Presses universitaires de France (PUF), 2020.

[26] Présidence de la République & ministère des Armées : *Revue stratégique de défense et de sécurité nationale*, 12 octobre 2017, DiCod (www.vie-publique.fr).

[27] Philippe Muller Feuga : « Extraterritorialité du droit : protection des intérêts stratégiques et réforme inachevée de la sécurité nationale », extrait d'intervention à l'Assemblée nationale, 17 juin 2019, Centre de réflexion sur la guerre économique, École de Guerre Économique (www.infoguerre.fr).

Mots-clés : influence, cyber, déstabilisation, information.