Cyber-influence : les nouveaux enjeux de la lutte informationnelle

Laure de Rochegonde, Elie Tenenbaum

Études de l'Ifri

Focus stratégique 104

CYBER-INFLUENCE

Les nouveaux enjeux de la lutte informationnelle

Laure DE ROCHEGONDE

Élie TENENBAUM

Mars 2021

Centre des études de sécurité

L'Ifri est, en France, le principal centre indépendant de recherche, d'information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l'Ifri est une association reconnue d'utilité publique (loi de 1901). Il n'est soumis à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux.

L'Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l'échelle internationale.

En partenariat avec

L'Observatoire des conflits futurs est un contrat-cadre pluriannuel d'études mené par un consortium réunissant la Fondation pour la recherche stratégique et l'Institut français des relations internationales sous le pilotage des trois états-majors d'armée

ISBN : 979-10-373-0320-2

Comment citer cette publication :

Laure de Rochegonde et Élie Tenenbaum, « Cyber-influence : les nouveaux enjeux de la lutte informationnelle », *Focus stratégique*, n° 104, Ifri, mars 2021.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tél. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

E-mail : accueil@ifri.org

Site Internet : Ifri.org

Focus stratégique

Les questions de sécurité exigent une approche intégrée, qui prenne en compte à la fois les aspects régionaux et globaux, les dynamiques technologiques et militaires mais aussi médiatiques et humaines, ou encore la dimension nouvelle acquise par le terrorisme ou la stabilisation post-conflit. Dans cette perspective, le Centre des études de sécurité se propose, par la collection ***Focus stratégique***, d'éclairer par des perspectives renouvelées toutes les problématiques actuelles de la sécurité.

Associant les chercheurs du centre des études de sécurité de l'Ifri et des experts extérieurs, ***Focus stratégique*** fait alterner travaux généralistes et analyses plus spécialisées, réalisées en particulier par l'équipe du Laboratoire de Recherche sur la Défense (LRD).

Auteurs

Élie Tenenbaum est chercheur au Centre des études de sécurité de l'Ifri et coordonateur du LRD. Il a publié de nombreux articles d'histoire et de stratégique sur les guérillas, le terrorisme et la contre-insurrection. Il est l'auteur de *Partisans et Centurions. Une histoire de la guerre irrégulière au XX^e^ siècle* (Perrin, 2018).

Laure de Rochegonde est chercheuse au Centre des études de sécurité de l'Ifri, où elle travaille sur la régulation des systèmes d'armes létales autonomes, et les négociations internationales autour du contrôle des armements avancés. Elle est en parallèle doctorante en science politique au Centre de recherches internationales (CERI) de Sciences Po Paris.

Comité de rédaction

Résumé

L'émergence d'une « info-sphère » numérique a considérablement modifié la nature de la stratégie militaire d'influence. Si les opérations d'information qui en découlent sont aussi anciennes que la guerre, les belligérants ont dû faire évoluer leurs stratégies en la matière, afin de s'imposer dans le cyberespace. Outre des acteurs non étatiques tels que l'État islamique y ayant recours dans une logique d'asymétrie, de grandes puissances comme la Chine, les États-Unis et la Russie se sont également montrées très actives en matière de lutte informationnelle dans le cyberespace. Dans un avenir proche, le développement de l'intelligence artificielle et des techniques de personnalisation, la modification de contenus ou l'emploi de la *blockchain* sont susceptibles de bouleverser la manière dont les armées appréhendent la guerre de l'information. Les transformations de ce domaine de lutte posent donc de nombreux défis aux armées, qui doivent s'adapter à une confrontation dépassant désormais leur cadre propre. À charge donc pour la France de prendre dès aujourd'hui la mesure de ces enjeux, et de mettre en œuvre un *aggiornamento* stratégique et capacitaire.

Abstract

The coming of age of a digital "info sphere" has dramatically changed the nature of military information support strategy. Though information operations are as old as war itself, armed forces have had to adapt their strategies to establish themselves in cyberspace. On the top of non-state actors such as the Islamic State using in its asymmetrical warfare way, great powers like China, the United States and Russia have been particularly active in this field of cyberspace information operations. In the near future, the development of artificial intelligence and personalization techniques, the modification of content or the use of blockchain are likely to disrupt even more the military approaches to information warfare. The transformation of this domain therefore poses many challenges to the armed forces, which must adapt to a confrontation that goes well beyond their ordinary scope. It is now up to France to get the measure of these issues, and to adapt accordingly in terms of strategy and capabilities.

Sommaire

Introduction

Le 10 novembre 2020, l'Arménie et l'Azerbaïdjan ont convenu d'un cessez-le-feu dans le Haut-Karabakh[1]. Si cet accord consacre la victoire sur le terrain des forces armées azéries, le conflit ne s'est pas déroulé uniquement dans le champ matériel. Les affrontements se sont accompagnés d'opérations de propagande, de désinformation et de piratage en ligne. Ainsi, le 27 septembre, le site d'information arménien *News.am* a été piraté afin de diffuser la fausse transcription d'un discours du Premier ministre Nikol Pashinyan exhortant les Arméniens à fuir le Haut-Karabakh, en raison des avancées de la « brutale armée azerbaïdjanaise[2] ». Le site pro-azéri *Defense.az* a en effet revendiqué le piratage de 90 sites arméniens par des hackers azéris, y compris ceux de *News.am* et de l'*Armenian Times*[3].

Ce type de campagne d'influence en ligne est devenu monnaie courante dans le paysage stratégique contemporain. Avant même de s'imposer dans le champ militaire, la « cyber-influence » avait démontré son potentiel dévastateur dans le monde politique, à l'occasion par exemple des élections présidentielles américaines (2016) et françaises (2017) ainsi que des référendums sur le Brexit (2016) et l'indépendance de la Catalogne (2017), qui avaient tous été perturbés par des campagnes de manipulation de l'information sur le Net. C'est la raison pour laquelle les États prennent très au sérieux l'enjeu que ces campagnes représentent. Le 14 juillet 2020, le chef d'état-major des armées reconnaissait dans une interview au *Monde* la préparation d'une doctrine de « lutte informationnelle dans le cyberespace », dont l'objectif sera de « lutter contre les tentatives de déstabilisation de l'information sur notre espace[4] ». Quelques semaines plus tard, le général Paul Nakasone, actuel directeur de la National Security Agency (NSA) et chef

Les auteurs souhaitent exprimer leur gratitude envers tous ceux qui ont rendu possible la publication de cette étude lors des entretiens de recherche conduits à l'automne 2020 ainsi que lors des diverses relectures. Ils remercient tous particulièrement Antoine Labarre et Claire Mabille qui les ont fidèlement assistés tout au long de la réalisation de ce rapport.

1. « Haut-Karabakh : Vladimir Poutine confirme un accord de 'cessez-le-feu' total entre l'Arménie et l'Azerbaïdjan », *Le Monde*, 10 novembre 2020.
2. E. Thomas et A. Zhang, « Snapshot of a Shadow War: A Preliminary Analysis of Twitter Activity Linked to the Azerbaijan-Armenia Conflict », *Quick take*, Canberra, Australian Strategic Policy Institute, octobre 2020.
3. « Azerbaijani Hackers Break into Over 90 Armenian Websites », *Defense.az*, 27 septembre 2020, disponible sur : http://defence.az.
4. N. Guibert, « Le général François Lecointre : 'une armée n'est pas faite pour la gestion de crise' », *Le Monde*, 14 juillet 2020.

du Cyber Command (CYBERCOM) déclarait que les opérations d'influence étrangères seraient le « prochain grand disrupteur[5] ».

De fait, l'environnement informationnel a profondément et durablement évolué sous l'impulsion des technologies numériques. Or la stratégie militaire d'influence, qui vise à « obtenir des effets sur les attitudes et les comportements en agissant sur les perceptions[6] », prend corps dans l'environnement informationnel. La tendance croissante à la numérisation se traduit alors par une porosité accrue entre l'espace informationnel et le cyberespace, que le ministère des Armées définit comme « l'espace de communication constitué par l'interconnexion mondiale d'infrastructures et d'équipements de traitement automatisé de données numériques et par les objets qui y sont connectés et les données qui y sont traitées[7] ».

La lutte informationnelle dans le cyberespace désigne dans cette perspective la stratégie militaire d'influence et les opérations d'information qui y sont conduites de façon autonome, ou en combinaison avec d'autres capacités cyber ou conventionnelles pour obtenir des effets militaires. Elle s'insère plus largement dans la problématique dite des « menaces hybrides » et de confrontation en « zone grise », c'est-à-dire sous le seuil de l'agression armée. L'influence, et tout particulièrement la lutte informationnelle, se range ainsi au tout premier plan des outils d'une stratégie indirecte qui, en l'état des rapports de force et des mécanismes de dissuasion, demeure la norme de la compétition stratégique entre puissance.

La présente étude s'attachera donc à appréhender la manière dont les armées peuvent faire face aux nouveaux défis posés par la lutte informationnelle dans le cyberespace, alors que celle-ci dépasse largement leur cadre propre. Le passage de l'influence à la cyber-influence (I) s'est décliné en stratégies diversifiées selon les puissances (II), qui augurent d'une intensification probable de ces procédés à l'avenir et à la lumière des évolutions technologiques, conduisant à un nécessaire *aggiornamento* stratégique pour les armées françaises (III).

5. S. Vavra, « NSA Director Ranks Influence Operations as a Top Concern », *Cyberscoop*, 16 septembre 2020.
6. *Stratégie militaire d'influence et opérations d'information*, DIA3-.10, CICDE, 12 mars 2018.
7. *Droit international appliqué aux opérations dans le cyberespace*, Ministère des Armées, Septembre 2019.

De l'influence à la lutte informationnelle dans le cyberespace

Aux origines de la stratégie d'influence

À bien des égards, les opérations d'influence sont aussi anciennes que la guerre elle-même. Carl von Clausewitz, dans son traité *De la guerre,* estime qu'il existe « deux facteurs inséparables » sur lesquels un belligérant doit peser pour faire plier son adversaire : « l'importance des moyens dont il dispose et sa force de volonté[8] ». Si l'action contre les moyens adverses par l'usage de la force a souvent été mise en avant dans l'histoire militaire, l'action sur sa volonté constitue un axe d'effort non moins négligeable. C'est précisément le but de la stratégie militaire d'influence que d'obtenir des effets sur la volonté de l'adversaire, notamment par le biais des informations auxquelles il a accès et à partir desquelles il forme ses perceptions, et prend ses décisions.

Cette action sur les perceptions peut être directe, en cherchant à influencer le chef militaire – en induisant en erreur ses capteurs et ses plans de guerre – ou plus indirecte, en s'exerçant sur ses responsables politiques, sa population civile et ses alliés, ou les acteurs neutres dont ses moyens peuvent dépendre. De même, elle peut être aussi bien offensive – influencer – que défensive – ne pas se laisser influencer.

Des perspectives tactiques : ruse et déception

Sur le plan tactique, et dans la perspective des combats entre belligérants, les procédés d'influence renvoient historiquement au domaine de la ruse. Aux côtés de la force et du courage, cette dernière est l'autre élément constitutif de l'art de la guerre[9]. Ces deux pôles étaient symbolisés dans la mythologie grecque par les figures divines d'Arès et d'Athéna, tandis qu'au Moyen Âge l'imagerie du lion et du renard était souvent mobilisée. Dans une perspective contemporaine, le terme de « déception » est employé de façon

8. C. von Clausewitz, *De la guerre*, traduit par Laurent Murawiec, Paris, Perrin, 2006, p. 41.
9. J.-V. Holeindre, *La Ruse et la Force. Une autre histoire de la stratégie*, Paris, Perrin, 2017.

plus précise et correspond à un mode d'action à part entière au sein de la stratégie militaire d'influence[10]. Il s'agit de tromper l'adversaire pour l'induire en erreur. La déception repose en principe sur trois activités, qu'il convient la plupart du temps de combiner.

La dissimulation est la plus classique. Il s'agit de cacher à l'adversaire sa manœuvre afin de le surprendre. Dans l'opération de déception la plus ancienne de la littérature qu'est le « cheval de Troie », les Grecs retirent leurs armées assiégeant la cité de la vue de leurs adversaires et cachent une petite équipe à l'intérieur de la structure de bois afin de faire croire faussement à un abandon du combat. Au fil des siècles, les méthodes de dissimulation n'ont cessé de se développer, pour inclure le camouflage, qui réduit la signature visuelle, mais également des procédés techniques comme la réduction de la surface équivalent radar.

La simulation consiste au contraire à exposer une manœuvre à des fins de diversion pour leurrer l'adversaire en lui faisant croire à une fausse situation. L'opération la plus connue dans ce domaine est bien entendu *Fortitude* en 1944, qui visait à faire croire à l'état-major allemand que les Alliés avaient l'intention de débarquer dans le Pas-de-Calais et non en Normandie. Pour ce faire, ils avaient simulé une armée d'invasion à partir de véhicules factices à proximité des points d'embarquement. Un tel stratagème est d'autant plus efficace qu'il s'accompagne d'un effort de dissimulation pour cacher la véritable manœuvre.

Dernier mode d'action de la déception, l'intoxication est une amplification de la simulation, visant à créer de la confusion chez l'adversaire, à perturber son processus de décision et à déstabiliser son organisation par la diffusion de fausses informations. De nombreux exemples existent là aussi, notamment dans les contextes où le renseignement et la sécurité opérationnelle sont déterminants, comme c'est le cas dans des conflits asymétriques face à des organisations clandestines dont la survie dépend de leur capacité à se prémunir contre l'infiltration. Ainsi lors de la guerre d'Algérie, le capitaine de 2e Bureau Paul-Alain Léger a mis au point une opération d'intoxication destinée à convaincre le chef de la Wilaya III (le maquis de Kabylie du Front de libération nationale), Amirouche Aït Hamouda, qu'il était massivement infiltré par des agents doubles. Il en a résulté une vague de « purges » sanglantes qui ont terriblement affaibli la Wilaya. Une autre opération d'intoxication communément employée consiste à opérer sous « fausse bannière » (*false flag*), à partir de « pseudo-unités » se faisant passer pour l'adversaire de

10. R. Hémez, « Opérations de déception. Repenser la ruse au XXIe siècle », *Focus stratégique*, n° 81, Ifri, juin 2018.

façon à lui imputer des actions dont les effets seraient négatifs – en termes d'image par exemple, ou simplement pour créer de la confusion dans les rangs ennemis. Plus que comme une ruse, ce type d'opération est considéré comme une « perfidie » par le droit des conflits armés, or cette dernière est illégale selon les conventions de Genève.

L'avènement de la guerre psychologique

La guerre n'est pas le seul domaine dans lequel l'information peut être manipulée – dissimulée, divertie ou fabriquée – afin d'obtenir un effet. Le champ politique mais aussi l'économie ou la religion ont souvent fait l'objet d'un antagonisme autour des perceptions. Or, ces domaines d'activité peuvent prendre une dimension stratégique dès lors qu'ils sont mobilisés dans le cadre d'un conflit armé. Ainsi, les guerres de religion qui ravagent l'Europe du XVI^e^ et XVII^e^ siècle voient le recours massif à divers procédés d'influence dans le champ théologico-politique, avec des conséquences directes dans des opérations militaires[11]. Le terme de propagande est ainsi né en 1622 lorsque, dans le cadre du Concile de Trente, le pape Grégoire XV fonde la « Congrégation pour la propagande de la foi » destinée à revivifier l'évangélisation catholique. Pour l'une des premières fois dans l'histoire, la capacité à persuader une population de la véracité d'un récit déterminerait l'issue d'un conflit armé.

La propagande peut s'accompagner de désinformation, qui vise à la diffusion de fausses nouvelles ou à la manipulation de l'information à travers une vision tronquée de la réalité. Cette dernière reprend les procédés déjà évoqués de l'intoxication, mais s'adresse à un auditoire plus large pour obtenir des effets politiques. Le terme lui-même apparaît à la fin du XIX^e^ siècle dans la Russie tsariste dont la police politique, l'*Okhrana*, se révèle friande – l'un des exemples les plus célèbres étant la diffusion du faux *Protocole des sages de Sion*, supposé révéler un complot pour la domination du monde par les Juifs et les francs-maçons.

C'est logiquement avec l'avènement de « l'âge démocratique » que la propagande gagne en importance en tant qu'arme de guerre. En Occident notamment, les masses de citoyens sont devenues une ressource cruciale par l'effet de la mobilisation – effectifs des armées, soutien moral et productif à l'arrière – et l'opinion publique exerce un poids grandissant sur la décision publique. Dès le mois d'août 1914, le Premier ministre britannique Lloyd George crée, sous la houlette du Foreign Office, un War Propaganda Bureau en charge notamment de convaincre l'opinion publique des pays neutres de

11. D. Crouzet et J.-M. Le Gall, *Au péril des guerres de religion : réflexions de deux historiens sur notre temps*, 1re édition, Paris, Presses universitaires de France, 2015.

soutenir l'Entente. En 1917, il ajoute un Department of Enemy Propaganda sous la responsabilité de Lord Northcliffe, magnat de la presse et fondateur du *Daily Mail*[12]. Ce dernier travaille à l'attaque du moral de l'ennemi allemand, non seulement au sein de ses forces armées mais aussi de sa population, tentant par exemple de diffuser l'idée que la guerre est perdue.

Les vecteurs pour exercer ces influences se diversifient. La rumeur et la circulation des journaux demeurent un facteur important comme le souligne Marc Bloch dans ses *Réflexions d'un historien sur les fausses nouvelles de la guerre* (1921), qui s'intéresse à la circulation des informations erronées des tranchées jusqu'à l'arrière, qu'elles soient le fruit de l'ennemi ou non. Mais de nouvelles techniques émergent également. Ainsi les Français auraient été les premiers à inaugurer le largage de tract par avion au-dessus des tranchées ennemies. Les Britanniques le pratiquent ensuite sur les populations allemandes dans le cadre de la *Papierkrieg,* que le général Ludendorff dénonce sans relâche dans son ouvrage sur la guerre totale. L'essor progressif de la radiodiffusion au début du XX^e^ siècle permet également de faire entrer la propagande de guerre au cœur des foyers.

La révolution bolchévique et la guerre civile qui s'ensuit en Russie augmentent encore l'importance de la propagande de guerre comme en atteste la création du Département pour l'Agitation et la Propagande (Agit-Prop) dès 1917. Ce dernier établit un contrôle étroit de la presse en imposant la *Pravda* comme principale source d'information, mais recourt également à la production culturelle (musique, théâtre, cinéma) pour enrôler les masses. Dans le domaine militaire, ces activités sont directement placées sous le contrôle de commissaires politiques, créés par Léon Trotski pour affermir son contrôle sur l'Armée Rouge. Ce modèle est exporté par les communistes chinois dès les années 1930 alors que Mao Zedong impose sa pratique de la guerre du peuple, qui mobilise les masses non seulement au moyen de la propagande mais aussi d'actions civiques auprès des populations[13].

La Seconde Guerre mondiale voit le renforcement de toutes ces méthodes. L'Allemagne nazie comme l'Italie fasciste ou encore l'URSS stalinienne recourent évidemment massivement à la propagande, mais les démocraties libérales ne s'en privent pas non plus, comme en atteste la création du ministère de l'Information au Royaume-Uni qui assure la censure de la presse et pilote les émissions de la BBC. Au contraire de ses homologues continentaux, cette dernière se distingue toutefois par une « politique de vérité » qui la conduit à ne jamais relayer de fausses informations – bien qu'elle présente l'actualité sous un angle favorable aux Alliés.

12. D. Colon, *Propagande : la manipulation de masse dans le monde contemporain*, Paris, Belin, 2019.
13. M. Zedong, *La Guerre révolutionnaire*, Paris, Éditions sociales, 1955.

Parallèlement, Londres procède à la création, au sein du ministère de la Guerre économique, d'un Special Operations Executive dont la fonction est de susciter la subversion et d'inciter à la révolte dans les territoires occupés. Ce dernier est composé en deux sections : le SO1 en charge de la propagande et le SO2 dédié au sabotage et au soutien paramilitaire aux bandes de partisans. Dès 1941, le SO1 s'autonomise pour prendre le titre de Political Warfare Executive (PWE). La « lutte politique » (*political warfare*) telle que la conçoivent les Britanniques dépasse donc la seule propagande pour inclure le soutien à des groupes subversifs impliqués dans diverses formes d'action politique – à l'instar de la campagne des « V », graffitis désignant le soutien à la cause alliée[14].

Avec l'entrée en guerre des États-Unis en 1941, le terme de « guerre psychologique » s'impose progressivement dans l'idée de mieux intégrer les différents échelons de la manœuvre d'influence, de la *political warfare* au niveau politico-stratégique jusqu'aux opérations sur le moral ennemi et la population au niveau tactique. La Psychological Warfare Division de l'état-major du général Eisenhower intègre ainsi pour la première fois des sections de « propagande de combat », qui accompagnent les unités combattantes au front et dans les zones libérées, et produisent des tracts adaptés à la situation, montent des organes de presse locaux, installent des émetteurs radio, etc.

Après 1945 et tout au long de la guerre froide, l'arme psychologique est institutionnalisée dans les armées occidentales. En 1952, l'US Army crée ainsi son 6e Groupe de radiodiffusion et de tracts, lequel commande à cinq compagnies tactiques dont certaines sont immédiatement envoyées en Corée pour appuyer l'action des forces. Ces dernières assurent les opérations psychologiques au niveau tactico-opératif tandis qu'au niveau politico-stratégique un Psychological Strategy Board coordonne l'action de diplomatie publique du Département d'État et de la *political warfare* de la CIA, dans un contexte d'affrontement idéologique entre les deux blocs.

Une évolution similaire a lieu en France, engagée militairement en Indochine face à un adversaire qui cherche à compenser son infériorité matérielle par la ruse, la déception et surtout la capacité à influencer et obtenir le soutien actif de la population, ainsi qu'à attaquer le moral du corps expéditionnaire, menant une guerre impopulaire à l'autre bout du monde. Pour contrer cette dynamique, les Français innovent, investissant dans les outils de propagande mais aussi dans des actions civilo-militaires dédiées à l'encadrement de la population.

14. D. Garnett, *The Secret History of PWE: The Political Warfare Executive, 1939-1945*, Londres, St Ermin's Press, 2002.

Ce modèle inspire l'état-major de la 10e Région militaire (Algérie) qui généralise la pratique des « 5e Bureaux » lesquels animent des organes de presse et de radio, organisent des projections cinématographiques et s'essaient à l'action sociale et politique – allant même jusqu'à organiser des manifestations[15]. Dans le *Texte Toutes Armes* n° 117 produit à l'été 1957, la doctrine française distingue la « guerre psychologique » menée contre l'adversaire de « l'action psychologique [...] qui s'adresse aux neutres et aux amis[16] ». Il s'agit alors pour l'armée française d'obtenir l'adhésion totale de la population algérienne au projet d'intégration à la République. Le bilan des 5e Bureaux reste toutefois mitigé : leur propagande semble souvent déconnectée des soucis des populations au quotidien, et leur action politique ne peut enrayer, d'un côté ou de l'autre de la Méditerranée, l'élan favorable à l'autodétermination.

Les enjeux de la communication stratégique

La guerre d'Algérie a démontré que l'action psychologique sur le seul théâtre d'opérations ne suffisait pas à influencer les perceptions de l'ensemble des acteurs. L'image négative de la guerre en France métropolitaine et à travers le monde pèse lourdement dans la décision du général de Gaulle de ne pas exploiter plus avant son avantage militaire. C'est à une problématique similaire que sont confrontés les Américains durant la guerre du Vietnam. Dans ce conflit, l'exécutif américain qui disposait jusqu'alors d'un solide soutien populaire dans toutes les guerres qu'il avait conduites perd pour la première fois la bataille de l'opinion. La couverture médiatique de la guerre, par la presse et la radio mais surtout par la télévision, qui s'impose désormais dans la majorité des foyers américains, est cruciale dans ce retournement. Les images non contrôlées d'une guerre lointaine, brutale, et de soldats désorientés, blessés ou traumatisés pèsent lourdement dans la mobilisation d'un mouvement anti-guerre qui devient majoritaire à partir de l'offensive du Têt en 1968.

Se pose alors avec une acuité toute particulière aux démocraties libérales la question du rapport des armées à des médias privés de plus en plus autonomes financièrement, qu'ils soient issus de leur propre pays ou de pays tiers. Les limites légales et éthiques en matière de liberté de la presse empêchent d'autant plus de manipuler ces derniers qu'il ne s'agit plus de guerre totale mais d'implications choisies dans des conflits menés au nom d'intérêts limités. La solution émerge au cours des années 1980 avec le développement de la communication institutionnelle et opérationnelle des

15. P. Villatoux et M.-C. Villatoux, *La République et son armée face au "péril subversif". Guerre et action psychologiques. 1945-1960*, Paris, Les Indes savantes, 2005.
16. « Instruction provisoire sur l'emploi de l'arme psychologique », *Texte Toutes Armes*, n° 117, juillet 1957.

armées, qui vise à valoriser l'action militaire auprès des médias, en mettant à leur disposition des éléments sélectionnés pour restreindre l'incitation de certains journalistes à s'informer auprès de l'adversaire[17].

La guerre du Golfe en 1991 consacre le succès de cette nouvelle approche, avec l'introduction de *pools* de journalistes étroitement encadrés par l'armée, qui les abreuve de conférences de presse et d'images exclusives. La concentration des groupes de presse privés et l'émergence de chaînes d'information continue de portée mondiale à travers des mastodontes tels que CNN rend d'autant plus aisée la stratégie de contrôle, qui peut se focaliser sur un champ bien structuré.

Avec les attentats du 11 septembre 2001 s'ouvre une nouvelle période, au cours de laquelle les États-Unis doivent combiner leur communication opérationnelle à une campagne intégrée d'influence stratégique contre l'idéologie djihadiste (« la guerre des idées ») déclinée au niveau tactico-opératif, sur les théâtres d'opérations tels que l'Afghanistan ou l'Irak, par un effort renouvelé dans le champ des opérations psychologiques. Cette période est toutefois marquée par l'affirmation de nouveaux médias non occidentaux tels qu'Al-Jazeera, disposant de leur propre accès aux sources d'information, ainsi que par la diffusion ou la fuite non contrôlée d'images ou de documents comme les photographies de la prison d'Abou Ghraïb en 2004, ou la publication par WikiLeaks de câbles militaires et diplomatiques en 2010. Ces événements, autant que le bilan décevant des opérations psychologiques dans le champ militaire, attestent d'une perte de contrôle de la communication des armées occidentales. Le phénomène d'horizontalisation de l'information s'accélère encore avec la généralisation des réseaux sociaux.

La réaffirmation au tournant des années 2010 d'une compétition stratégique accrue entre puissances globales et régionales est encore venue renforcer la problématique de l'influence. Parallèlement au développement continu des réseaux sociaux et de « l'info-sphère », la mise en œuvre par la Russie, la Chine et d'autres pays d'une posture beaucoup plus virulente, aussi bien dans le champ de la communication, de la diplomatie publique, que dans celui de la manipulation de l'information – le cas échéant appuyée par des moyens d'action clandestine – a engendré un contexte où l'influence fait figure d'instrument central d'une stratégie plus large de « zone grise ».

17. T. Rid, *War and Media Operations: Tthe U.S. Military and the Press from Vietnam to Iraq*, New York, Routledge, 2007.

Stratégie militaire d'influence et opérations d'information

Sous l'influence des États-Unis et à l'aune de plusieurs expériences opérationnelles telles que celles des missions de maintien de la paix dans les Balkans ou de la Force internationale d'assistance à la sécurité (FIAS) en Afghanistan, la plupart des armées des États membres de l'Organisaion du traité de l'Atlantique nord (OTAN) se sont aujourd'hui approprié les enjeux de communication stratégique. D'après la doctrine OTAN, la communication stratégique (StratCom) est désormais le concept intégrateur par excellence, qui vise à mettre en cohérence l'action et le discours du pays qui la pratique dans toutes ses composantes : ses activités militaires comme sa diplomatie publique, voire sa politique intérieure. Cette mise en cohérence se situe en principe au plus haut niveau de l'exécutif afin de garantir une approche globale et en principe interministérielle.

La StratCom se décline ensuite en deux composantes. La première relève de la communication institutionnelle, et notamment la diplomatie publique (pour les audiences étrangères) et les affaires publiques (pour la scène intérieure). Dans le champ militaire, celle-ci peut ensuite donner lieu à une forme de communication opérationnelle au plus près du théâtre. Toutes deux sont tournées vers la valorisation de l'action militaire auprès du public, des médias, ainsi que des décideurs (représentation parlementaire, partenaires étrangers). Il ne s'agit pas de produire un effet militaire opérationnel au profit de la force ou de l'état final recherché – même si la communication y contribue indirectement.

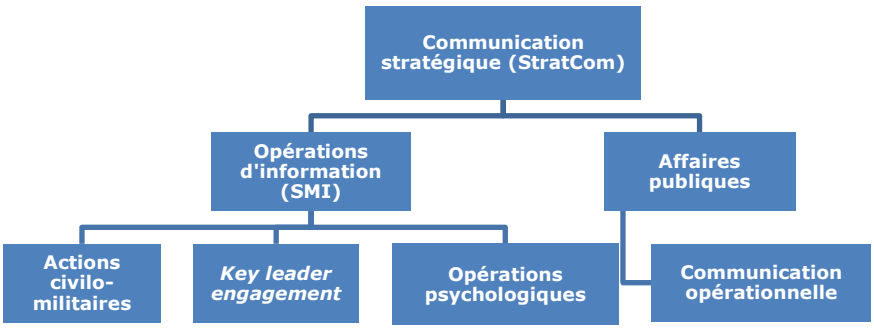
Il en va autrement de la seconde branche de la StratCom qui renvoie aux opérations d'information et à la stratégie militaire d'influence (SMI), plus intégrées à la manœuvre et qui visent à affecter les perceptions, la compréhension et la volonté, donc *in fine* le comportement des acteurs (adversaires, alliés ou neutres) d'un conflit dans le sens de l'état final recherché. Concrètement, ces opérations d'information consistent à synchroniser les actions d'information procédant d'une double finalité, d'une part la guerre de commandement et de contrôle, d'autre part l'influence sur les « audiences cibles » du théâtre, par des moyens non létaux. À cet égard, les procédés de déception (*cf. supra*) peuvent s'insérer dans la SMI, même si celle-ci peut viser d'autres objectifs que de tromper ou d'intoxiquer l'ennemi : le décrédibiliser auprès de ses soutiens, gagner l'appui et la confiance de la population voire de certaines forces d'opposition en favorisant des ralliements, renforcer le moral et la cohésion des forces amies sont autant d'objectifs possibles de la SMI.

La doctrine otanienne reconnaît à ce jour trois principaux types d'opérations d'information pour ce qui est de l'influence. Le premier relève de la coopération civilo-militaire (CIMIC) : lointaine descendante des unités « d'affaires civiles » ou encore de pacification pour administrer les territoires récemment conquis, ces missions travaillent en principe à l'amélioration de certaines conditions sociales ou économiques sur la zone d'opération et, ce faisant, contribuent à l'acceptation de la force, à une perception positive de son action et à la coopération de la population – y compris en termes de renseignement.

Le second type d'opération est désigné par l'expression anglophone de « *key leader engagement* » (KLE) qui désigne le travail d'influence, direct ou indirect, auprès des chefs civils ou militaires sur un théâtre donné. Fortement empreinte elle aussi des expériences contre-insurrectionnelles d'Afghanistan et d'Irak, le KLE est une version ciblée et personnalisée du CIMIC visant à accroître la confiance et la qualité de la coopération avec les acteurs locaux, valorisant ainsi les corps intermédiaires (chefs traditionnels, autorités religieuses, acteurs économiques, etc.) directement en prise avec la population.

Enfin les opérations psychologiques (PSYOPS) à proprement parler constituent le troisième axe. D'une nature plus spécifiquement informationnelle, elles se définissent par la formulation et la diffusion de messages destinés à changer, maintenir ou renforcer les perceptions d'individus ou d'organisations collectives.

Schéma n° 1 : L'influence dans la doctrine OTAN



Source : AJP 3.10

Comme toute approche opérationnelle, la stratégie militaire d'influence repose sur un cycle de décision. Il faut d'abord analyser les enjeux à l'aune de l'état final recherché, avant d'identifier les auditoires qui seront ciblés en priorité, puis de formuler un contenu (ou « charge informationnelle ») apte à peser sur ces perceptions. De cette modalité dépend également le choix du

degré d'attribution du message et des vecteurs de diffusion, ainsi que de son éventuelle amplification.

La connaissance de l'environnement informationnel (la recherche, le recueil et l'analyse) est naturellement indispensable à l'élaboration d'une opération d'information. Cette fonction dépend largement de la nature de la cible. Il peut s'agir d'une organisation militaire ennemie ou d'un groupuscule extrémiste comme de la population plus large d'un théâtre – avec un traitement, là encore, différencié selon qu'elle appartient à une société ouverte où les informations circulent aisément ou au contraire à un État autoritaire contrôlant étroitement les échanges. En fonction de ces caractéristiques, les renseignements pourront provenir d'un processus de recherche plus ou moins ouvert, mobilisant des moyens plus ou moins complexes. La dimension psychologique et sociale demeure toutefois un enjeu essentiel, mobilisant ainsi presque toujours des compétences issues des sciences humaines (psychologie, sociologie, linguistique, etc.).

Ce travail d'analyse et d'identification terminé, vient le temps de la formulation du contenu ou de la « charge informationnelle ». Quel message cherche-t-on à faire passer et dans quel but ? Il peut s'agir de valoriser une cause ou au contraire de la dénoncer, de démoraliser l'adversaire et de le diviser, de susciter des désertions, d'inciter une population à coopérer, etc. Les méthodes sont variées et peuvent aller de la diffusion d'une information discrète qui se propagera par son seul contenu, à une campagne orchestrée suivant les principes classiques du marketing. On retrouve ainsi les procédés visant à capter l'attention (émotion, personnalisation, divertissement, surprise, humour) et emporter l'adhésion (simplification, exagération, vraisemblance) de la cible[18]. Ces techniques peuvent être amplifiées par des méthodes de propagande, comme la répétition du message jusqu'à saturation, ou la suppression des sources alternatives et des messages discordants. Enfin, les opérations d'information peuvent employer des techniques extrêmes telles que l'endoctrinement (destruction cognitive suivie d'un processus de reconstruction mentale) ou la terreur (généralement associée à la menace de recours à des formes de violence extrême), toutes deux réalisées sous fortes contraintes physiques et en dehors de tout cadre éthique ou juridique internationalement accepté.

Directement associée au contenu se pose la question de l'attribution. Les spécialistes de la guerre psychologique distinguent traditionnellement entre information blanche, grise et noire. L'information blanche est ouvertement attribuée à son auteur, tandis que l'information grise n'est pas revendiquée. L'information noire enfin est faussement attribuée à un autre

18. V. de Barnier et H. Joannis, *De la stratégie marketing à la création publicitaire*, Paris, Dunod, 2010.

auteur (« fausse bannière »). La stratégie d'attribution dépend logiquement du contenu : si une offre d'amnistie gagne à être signée formellement de celui qui la formule, une tentative d'intoxication ou de désinformation ne peut être attribuée sans se retourner contre son auteur.

En ce qui concerne le contenu du message, la France et le reste des armées de l'OTAN se fixent dans leur doctrine des limites claires sur le plan éthique et juridique. La véracité et l'attribution demeurent la norme recommandée dès lors que ces opérations, comme toute action militaire, engagent la responsabilité de leurs États. Cela ne signifie pas que d'autres modes d'action ne puissent pas être employés par d'autres services versés dans les opérations clandestines.

Enfin, une fois le message formulé vient l'étape de sa diffusion. Les vecteurs sont divers. La doctrine distingue en principe les actions médiatiques et les actions hors-médias. Ces catégories tendent toutefois à se confondre avec la convergence numérique.

- **Actions médiatiques** : presse, radio, télévision. Il peut s'agir de productions écrites ou audiovisuelles originales (les unités de PSYOPS disposent de moyens de production propres) et diffusées par des moyens nationaux – à l'instar de Voice of America pour les États-Unis ou RT pour la Russie – voire par des moyens militaires, potentiellement liés à des moyens de guerre électronique à l'instar de EC-130J Commando Solo de l'US Air Force capable d'émettre dans les bandes FM ou TV pour diffuser des messages sur des ondes locales.

  Lors de la guerre en Irak de 2003, l'unité a ainsi réussi à insérer sur les ondes de la télévision irakienne un message du président Bush exhortant la population à renverser Saddam Hussein. Ces productions écrites ou audiovisuelles peuvent aussi passer par des médias externes, *via* l'achat de temps d'antenne par exemple. Ainsi en 2002, les États-Unis ont lancé pour un budget de 15 millions de dollars la campagne « Shared Values » consistant à diffuser des spots publicitaires soulignant les convergences morales entre l'islam et l'Amérique sur les chaînes de télévision de plusieurs pays musulmans.

  Enfin, une action plus indirecte, coordonnée avec la communication opérationnelle, consiste à fournir des informations à des médias indépendants qui les relayeront avec plus ou moins de distance.

- **Vecteurs « hors média »** : le contact direct continue à jouer un rôle important pour peser sur les perceptions. La participation à de grands événements, meetings, défilés, spectacles et concerts, voire cérémonies religieuses demeure un vecteur employé par de nombreux acteurs. Elle peut naturellement se combiner à des relais *ad hoc*. Si par le passé

l'utilisation de haut-parleurs ou le largage aérien de tracts ont compté parmi les vecteurs phares de la guerre de l'information, ces possibilités sont aujourd'hui complétées par le contact par courrier électronique ou encore par téléphone et SMS – procédé massivement employé par les forces russes contre les soldats ukrainiens depuis 2014, ou l'armée israélienne lors de ses opérations à Gaza en 2009 et 2014.

La lutte informationnelle dans le cyberespace

Dans le domaine de l'influence comme ailleurs, la révolution numérique modifie radicalement les usages. Elle transforme la manière dont l'information est produite, distribuée et consommée. À l'échelle des sociétés civiles, les populations s'informent sur les médias sociaux et reçoivent des newsletters par mail. D'après le *Digital News Report 2020* du Reuters Institute, une personne sur deux dans le monde déclare s'informer sur les réseaux sociaux, et l'attrait pour les newsletters a significativement augmenté l'année dernière[19]. Même les médias traditionnels (presse, radio, télévision) sont désormais presque intégralement numérisés : les journaux se sont dotés d'applications dédiées, les signaux TV et radio sont eux-mêmes numérisés, tandis que l'écoute et le visionnage différés en ligne par *podcast* et *replay* séduisent de plus en plus d'adeptes (ils étaient respectivement 4,3 et 7,8 millions en France en 2019[20]). Sous une forme ou une autre, l'information est donc désormais largement numérisée, en même temps que l'espace où sont façonnées les perceptions.

Ce constat s'applique également au domaine militaire où les systèmes d'information et de commandement comme les systèmes d'armes se reposent dans leur grande majorité, sinon leur totalité, sur des technologies numériques[21]. Cette tendance croissante à la numérisation se traduit alors par une convergence accrue entre l'espace informationnel et le cyberespace.

Il est convenu de se représenter ce dernier sous la forme de trois couches : une physique ou matérielle, qui recouvre les équipements et les infrastructures (câbles, serveurs, terminaux, etc.), une logique, constituée par les données numériques et les moyens de les transmettre dans les réseaux (protocoles, applications, interfaces, etc.) et enfin une couche sémantique ou cognitive constituée par « les informations qui circulent dans

19. N. Newman *et al., Digital News Report 2020*, Oxford, Reuters Institute for the Study of Journalism, juillet 2020.
20. *L'année TV 2019 : les nouveaux défis d'un média innovant*, Médiamétrie, 23 janvier 2020.
21. O. Becht et T. Gassilloud (rapporteurs), *Rapport d'information sur les enjeux de la numérisation des armées*, Rapport n° 996, Paris, Commission de la défense nationale et des forces armées, Assemblée nationale, mai 2018.

le cyberespace et par les personnes qui peuvent disposer de multiples identités numériques ou « avatars » (pseudonymes, adresses de messagerie, adresses IP, *blogs*, etc.)[22]. C'est à partir de cette dernière couche que sont conduites les opérations de lutte informationnelle dans le cyberespace, dans le cadre de la stratégie militaire d'influence.

Un nouveau domaine de lutte

En première analyse, il est courant de ne considérer le cyberespace que comme un vecteur de la stratégie militaire d'influence, au même titre que l'écrit, la radio ou la télévision. Cette approche semble néanmoins beaucoup trop restrictive au regard de son caractère englobant d'une part, mais aussi de ses caractéristiques techniques et sociales d'autre part, qui transforment en profondeur la manière de concevoir une stratégie d'influence.

La globalisation et l'immédiateté sont sans doute les premières caractéristiques frappantes du cyberespace. L'immédiateté résulte de la circulation électronique de l'information, et la globalisation de l'interconnexion des réseaux. Il en découle que le cloisonnement des théâtres qui pouvait encore exister avant la numérisation totale de l'information est de moins en moins envisageable. S'il est toujours possible de cibler un auditoire donné, les planificateurs doivent désormais partir du postulat que le message peut se diffuser bien au-delà du public initialement visé.

Des limites existent à cette impression de fulgurance et de porosité complète. La première est celle de la langue qui demeure, en dépit des progrès en matière de traduction automatique, un frein important à la circulation d'une information. Et pour cause : la traduction peut aussi être l'occasion d'une mésinformation (involontaire) ou d'une manipulation de l'information comme a pu l'illustrer par exemple le mouvement anti-français de l'automne 2020 au cours duquel la dénonciation du « séparatisme islamiste » par le président Macron a pu apparaître comme une attaque contre l'islam en général à la faveur de mauvaises traductions[23].

Une autre limite à la globalisation du cyberespace tient aux régimes juridiques qui lui sont associés et au lien que ceux-ci entretiennent avec les États qui les imposent. Le cyberespace a ainsi été marqué historiquement par une forte polarisation américaine, sur les plans économique et technologique. Les révélations d'Edward Snowden ont démontré, si besoin était, le lien entre les services de renseignement américains et les grandes plateformes du web employées globalement. Conscientes de cette situation, la Russie comme la

22. « Éléments publics de doctrine militaire de lutte informatique offensive », nr.101000/MINARM, 2018.
23. « 'Séparatisme' : En Égypte, Al-Azhar qualifie de 'racistes' les propos de Macron », *RFI*, 5 octobre 2020.

Chine ont travaillé depuis le début des années 2000 à l'édification d'un « Internet souverain[24] » aussi bien dans ses « couches basses » (serveurs, protocoles, etc.) que dans ses plateformes (réseau social, messagerie, etc.), afin notamment de mieux contrôler les influences étrangères. Les opérations d'information doivent donc prendre en compte une nouvelle géographie numérique particulièrement complexe sur le plan du droit, mais aussi des capacités techniques d'interdiction (à l'instar du « grand *firewall* » chinois).

La personnalisation et l'opacité sont deux autres caractéristiques propres au cyberespace qui transforment lourdement la pratique des opérations d'information. En effet, si le cyberespace – surtout depuis l'avènement des réseaux sociaux – est marqué par une forte personnalisation de l'expérience de l'utilisateur à travers le développement de profils accumulant des métadonnées de plus en plus complètes, l'identité numérique (avatar) demeure essentiellement déclarative, ce qui rend beaucoup plus aisé le recours à des identités fictives. L'opacité est donc bien un corollaire de cette hyperpersonnalisation dans laquelle les identités sont en fait sujettes à construction. L'anonymat et l'impunité relative auquel il donne accès ont ainsi joué un rôle clé dans l'inflation des fausses informations ou des propos haineux, dont le web social est devenu la principale caisse de résonance. Ces deux aspects facilitent aussi l'emploi d'opérations en zones grises.

Les pratiques de la « propagande noire » et de l'intoxication sous fausse bannière peuvent aussi plus aisément bénéficier du vol ou de l'usurpation d'une identité numérique – généralement après une intrusion ou un piratage informatique (*hacking*). De même, la diffusion d'informations grises sous forme de rumeurs sur les réseaux semble particulièrement attractive. Même l'information blanche paraît avoir gagné en opacité *via* le principe du « *one click attributed* » consistant à diffuser un contenu dont l'attribution n'apparaît qu'après que l'utilisateur a fait la démarche de suivre un lien hypertexte[25].

L'horizontalité et l'interactivité constituent également des spécificités du cyberespace, tout particulièrement depuis l'avènement au début des années 2000 du web social, ou « 2.0 ». Chaque consommateur d'information y est dorénavant aussi un producteur et un diffuseur potentiel. Il existe une grande porosité entre les plateformes des réseaux sociaux, des médias traditionnels (à travers les commentaires), des forums de discussion ou des applications de messagerie. Il en découle une circulation de l'information

24. J.-C. Noël, « Qu'est-ce que la puissance numérique ? », *Études de l'Ifri*, Ifri, novembre 2019.
25. T. C. Helmus *et al.*, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, Santa Monica, CA, RAND Corporation, 2018.

marquée par la « viralité » qui vient encore accélérer la vitesse des communications.

Différents outils sont utilisés pour diffuser, mettre en valeur, alimenter et amplifier les contenus. Le procédé le plus connu est celui des « trolls » qui relayent et commentent des contenus de façon plus ou moins compulsives et systématiques. Ils peuvent également pratiquer le cyber-harcèlement, par le biais de blocages intempestifs, de propos injurieux ou de menaces. Ces méthodes peuvent aussi inclure la traque sur Internet (*stalking*) et éventuellement le vol par intrusion (*hacking*) de toute information compromettante et leur révélation (*outing*) en vue du dénigrement et de la diffamation d'un adversaire.

Afin d'accroître la viralité de ces actions, les acteurs du cyberespace peuvent recourir à des procédés d'amplification. Certains sont mis à disposition des utilisateurs par les plateformes elles-mêmes, comme la pratique du mot-dièse (*hashtag*) destiné à faciliter le suivi et la visibilité d'une thématique sur Twitter ou Facebook, ou encore le recours au *sponsoring* consistant à payer pour promouvoir un contenu, en ciblant éventuellement un auditoire précis renseigné grâce aux métadonnées. C'est le procédé employé par l'entreprise Cambridge Analytica, qui a orchestré en 2016 des campagnes de marketing politique controversées en faveur du « non » lors du référendum sur le Brexit au Royaume-Uni, et de soutien au candidat Donald Trump lors de l'élection présidentielle américaine la même année.

D'autres méthodes d'amplification dites « inauthentiques » existent, tels que les comptes automatisés (*bots*), employés pour partager ou valoriser (*likes*) systématiquement certains contenus. Facilement repérés par les algorithmes de régulation lorsqu'ils sont rudimentaires, les *bots* peuvent être sophistiqués par le biais de l'intelligence artificielle (IA) ou être occasionnellement opérés par des humains (cyborgs) afin de mieux simuler un comportement authentique. D'une manière générale, l'association du *trolling* et des *bots* peut permettre ponctuellement de créer l'impression d'une opinion majoritaire sur un sujet donné. Cette technique consistant à simuler la popularité, en faisant croire à un mouvement social citoyen (*grassroot movement*), est appelée *astroturfing*, en référence à une compagnie (AstroTurf) de pelouse artificielle[26].

Enfin, la dernière caractéristique du cyberespace en matière d'influence tient à sa plasticité, c'est-à-dire à la facilité d'y créer, noyer, ou modifier un ensemble de contenus. La modification et le détournement de contenus comptent parmi les pratiques les plus anciennes de la lutte informationnelle

26. J.-B. Jeangène Vilmer *et al.*, *Les manipulations de l'information, un défi pour nos démocraties*, CAPS, IRSEM, août 2018.

dans le cyberespace, et recoupent largement d'autres procédés de lutte informatique offensive (LIO) visant par exemple au sabotage de certains systèmes d'information. Bien qu'elles s'appuient sur des ressorts techniques, ces opérations sont susceptibles de produire des effets cognitifs.

Les attaques par déni de service et déni distribué (DoS et DDoS) consistent à surcharger les serveurs de requêtes, pour empêcher l'accessibilité d'une plateforme. Plus sophistiquées, les intrusions permettent de modifier les contenus provoquant le « défacement » d'un site web et l'usurpation de comptes sur les réseaux sociaux. C'est le procédé utilisé par exemple lors de l'attaque contre la chaîne de télévision francophone TV5 Monde en avril 2015 au cours de laquelle la diffusion de la chaîne est interrompue durant 22 heures tandis que des messages de soutien à l'État islamique (EI) et des documents présentés comme des plans opérationnels et des adresses et CV de militaires impliqués dans la lutte contre le terrorisme sont publiés sur ses comptes Facebook et Twitter[27].

L'intrusion peut également avoir pour objet le vol de données suivi de leur révélation (*hack and leak*), comme ce fut vraisemblablement le cas lors de l'attaque contre la Convention nationale démocrate (DNC) américaine en 2016, au cours de laquelle des e-mails ont été volés et ont ensuite fuité auprès des sites DC Leaks et WikiLeaks qui les ont diffusés. Cette opération a d'ailleurs été suivie d'une campagne d'amplification, portée par certains soutiens du parti républicain [28].

Enfin, la plasticité du cyberespace a également démocratisé la pratique ancienne des faux documents, *via* la modification d'images – ou plus simplement encore de légendes d'images – et la fabrication de documents, d'articles ou des sites Internet destinés à tromper ou créer du doute chez la cible. Ces procédés peuvent s'hybrider, et ainsi la diffusion d'un faux prendre l'apparence d'une fuite à scandale (*outing*) comme dans le cas des « Macron Leaks » survenues pendant les élections présidentielles françaises en 2017[29].

Les enjeux militaires de la cyber-influence

Dans leur majorité, les actions de lutte informationnelle dans le cyberespace, y compris dans le cadre de conflits armés ouverts et militarisés, ont jusqu'à présent été employées au niveau politico-stratégique, dans une perspective de modelage (*shaping*) de l'environnement informationnel. Si les armées

27. A.-L. Frémont, « Piratage de TV5 Monde : mystère autour de l'identité du « CyberCaliphate » », *Le Figaro*, 9 avril 2015.
28. R. S. Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, Washington, D.C., US Department of Justice, mars 2019.
29. S. Halimi et P. Rimbert, « Après le rapport Mueller, le fiaso du 'Russiagate', Tchernobyl médiatique », *Le Monde diplomatique*, 1er mai 2019.

sont impliquées, il s'agit avant tout de peser sur la perception générale du conflit par les populations et les acteurs, la mise en récit politique, etc. Il est toutefois possible de dégager des enjeux plus spécifiquement militaires aux opérations d'information dans le cyberespace. Ces dernières peuvent être rangées en deux grandes catégories : les actions de déception contre une force adverse et les actions sur l'environnement humain d'une force.

Les actions de cyber-déception reposent sur les mêmes procédés que ceux de la déception classique : il s'agit toujours de cacher, simuler ou intoxiquer l'adversaire. Dès lors que les forces armées comme les groupes irréguliers utilisent des systèmes numérisés pour communiquer, ceux-ci s'exposent à une intrusion et une manipulation. L'opération israélienne *Orchard* visant en 2007 un réacteur nucléaire en construction dans la région de Deir ez-Zor semble avoir démontré l'efficacité d'une attaque informatique contre le système de surveillance aérienne syrien pour dissimuler la pénétration des avions de combat. Dans ce cas cependant, la dimension informationnelle s'est limitée à la perception des opérateurs radars, l'essentiel de l'effet ayant reposé sur les procédés techniques d'intrusion et de neutralisation de tout ou partie du système de commandement et de contrôle syrien. Il est toutefois possible d'envisager des manipulations plus complexes, comme la simulation d'une fausse attaque après la compromission d'un système de suivi des forces amies (*blue force tracking*) voire après l'intrusion au sein d'un système de commandement, l'usurpation de l'identité d'une haute autorité de théâtre détournant les ordres opérationnels envoyés aux unités.

Si de telles actions sont particulièrement difficiles à mettre en œuvre face à un adversaire utilisant un système durci non connecté à Internet – sa pénétration exige alors souvent le recours à des moyens avancés de guerre électronique et/ou de renseignement humain – elles sont plus aisées face à des groupes irréguliers se reposant sur des moyens de communication certes cryptés, mais plus faciles d'accès, tels que les messageries électroniques. Ensuite, pour usurper de façon crédible une identité numérique, des méthodes existent, dérivées des techniques de User Behavioral Analysis (UBA) qui permettent, à partir de l'exploitation des métadonnées, d'identifier un *pattern* comportemental propre à un individu ou à une organisation, et ainsi à simuler efficacement un comportement authentique.

Face à la difficulté de pénétrer un système de commandement opérationnel, la déception militaire peut rechercher d'autres voies d'influence sur la force adverse en exploitant des domaines de moindre vigilance des utilisateurs en termes de sécurité opérationnelle. L'une de ces vulnérabilités, aujourd'hui bien identifiée mais non moins persistante, renvoie par exemple à la présence des combattants sur les réseaux sociaux à titre privé. Ils

peuvent ainsi faire l'objet de campagnes d'influence sur leurs comptes personnels, comme l'ont été des soldats ukrainiens qui ont reçu des messages visant à altérer leur moral ou leur cohésion, leur annonçant par exemple qu'ils étaient « encerclés et abandonnés[30] ».

Ainsi, dans une opération de déception documentée par le Modern War Institute de West Point, des familles de soldats ukrainiens d'une même unité ont reçu simultanément un SMS annonçant leur décès, suscitant des appels en retour de ces mêmes proches, permettant ainsi, par la concentration de signaux, de repérer leur position pour les bombarder[31]. Dans une même perspective, on pourrait évoquer l'utilisation par le Hamas palestinien de faux profils sur une application de rencontres en ligne ciblant systématiquement des jeunes hommes posant en uniforme sur leur profil et leur donnant des rendez-vous qui se révélaient être des guets-apens pour les kidnapper[32]. On peut enfin citer l'utilisation par des soldats américains et français de l'application d'analyse de performances sportives Strava, qui a entraîné la fuite sur Internet de la localisation de plusieurs bases militaires en Irak et au Niger, les données de course étant géolocalisées[33].

Les actions sur l'environnement humain d'une force constituent le second angle possible d'opérations d'information spécifiquement ciblées sur le champ militaire. Toujours suivant la logique de la ligne de vulnérabilité maximale, il peut en effet être plus aisé de s'attaquer à l'environnement humain d'une force – et tout particulièrement aux populations civiles environnantes – qu'à la force. En janvier 2017, le parquet lituanien a par exemple reçu un e-mail au sujet du viol présumé (et inventé) d'une adolescente par des soldats allemands déployés dans le cadre de l'*enhanced Forward Presence* (eFP) dans la ville de Ruklan, au nord-ouest de Vilnius. S'en est suivie une campagne de manipulation de l'information cherchant à dégrader l'image de la force[34]. Un autre exemple est l'organisation en août 2018 d'une manifestation hostile ayant encerclé le camp des Forces françaises de Côte d'Ivoire à Lomo-Nord, près de Yamoussoukro, pour s'opposer à un exercice de tir au canon CAESAR. Les manifestants craignaient que les munitions ne soient « composées de bombes et d'éléments radioactifs [...] nuisibles pour la santé », une information évidemment fabriquée de toutes pièces et véhiculée sur les réseaux par des

30. L. Collins, « Russia Gives Lessons in Electronic Warfare », Association of the United States Army, 26 juillet 2018, disponible sur : www.ausa.org.
31. *Ibid.*
32. Entretien avec un officier des Forces de défense israéliennes, Tel Aviv, janvier 2019.
33. N. Six, « Une application de jogging menace la sécurité des bases militaires », *Le Monde*, 29 janvier 2018.
34. L. Lagneau, « Angela Merkel dénonce la 'guerre hybride' de la Russie contre les soldats allemands déployés en Lituanie », *Opex360*, 16 septembre 2018, disponible sur : www.opex360.com.

trolls russes[35]. Dans un cas comme dans l'autre, la diffusion de ces fausses informations a contribué à tendre les relations d'une force étrangère avec la population. En fonction de la réponse qui y est apportée, ces tensions peuvent s'objectiver et prendre une tournure irrémédiable, risquant de remettre en cause la mission elle-même.

35. P. Airault, « Armée française en Afrique : péril en la demeure », *L'Opinion*, 21 août 2018.

Des stratégies de cyber-influence diversifiées

Les grandes puissances aussi bien que les belligérants non étatiques pratiquent aujourd'hui, sous une forme ou une autre, la lutte informationnelle dans le cyberespace. Les moyens, méthodes et organisations varient toutefois grandement selon les acteurs. Nébuleuse d'acteurs contraints à l'action asymétrique par leur infériorité matérielle, la mouvance djihadiste internationale tout d'abord, a fait de la cyber-influence l'une de ses armes essentielles pour rééquilibrer son combat contre ses adversaires désignés, évoluant d'un simple usage de propagande vers une subversion plus ambitieuse. Outre ces organisations non étatiques, trois États se distinguent par leur emploi massif de la cyber-influence, dont certains exemples ont été largement documentés. Les États-Unis, la Russie et la Chine sont les puissances les plus actives en termes d'opérations d'influence dans le cyberespace. En dépit de points de comparaison, leurs stratégies de cyber-influence diffèrent néanmoins. Alors que les États-Unis mettent en œuvre une vaste convergence cyber-informationnelle, la Russie s'appuie sur des relais plus clandestins. La Chine a quant à elle bâti un appareil de contrôle souverain et d'influence extérieure à la mesure de ses ambitions globales.

Djihadisme : de la propagande en ligne au cyber-terrorisme

L'action terroriste trouve sa place parmi les outils de la stratégie d'influence : à bien des égards, l'attentat est d'abord et avant tout un acte de « propagande par le fait » destiné à faire connaître une cause – ou éventuellement à provoquer une réaction inadaptée de la part de l'adversaire permettant ensuite de transformer les conditions politiques en faveur du mouvement[36]. Le succès du terrorisme, et tout particulièrement tel qu'il émerge à partir du milieu des années 1970, dépend profondément de la façon dont les nouveaux médias globalisés acceptent – ou non – de se faire la caisse de résonance de

36. C'est notamment la logique proposée par le révolutionnaire Carlos Marighella dans son *Mini-manuel de guérillla urbaine*, publié en 1968. Sur les passerelles existant entre le terrorisme révolutionnaire et le terrorisme djihadiste lire, parmi d'autres, G. Chaliand, *Terrorismes et guérillas : techniques actuelles de la violence*, Paris, Flammarion, 1985 ; M. Hecker, « De Marighella à Ben Laden: Passerelles stratégiques entre guérilleros et djihadistes », *Politique étrangère*, 2006, Été, nº 2, p. 385.

son action. Des nationalistes palestiniens à l'ultra-gauche révolutionnaire allemande ou italienne comptaient avant tout sur la publicité médiatique de leur action pour susciter une réponse politique. C'est dans cette ligne que se situe à bien des égards la mouvance djihadiste internationale qui émerge dans les années 1990 autour des anciens combattants étrangers partis combattre les Soviétiques en Afghanistan.

Consciente de sa dépendance à l'égard des grands médias, la nébuleuse djihadiste en a aussi vite ressenti les limites, au fur et à mesure que ces derniers se faisaient moins complaisants à son égard. Si Oussama Ben Laden a été friand d'interviews données à des journalistes occidentaux dans les années 1990, les attentats du 11 septembre 2001, la traque contre sa personne et la guerre globale déclenchée contre son organisation marginalisent considérablement son accès aux grands médias et donc ses moyens d'influence. Dans la première décennie des années 2000, al-Qaïda est encore largement dépendante des rares organes de presse qui acceptent de diffuser ses messages, essentiellement la chaîne d'information qatarie al-Jazeera, qui se montre de plus en plus sélective dans la diffusion des « cassettes » audio et vidéo qui sont envoyées à sa rédaction.

C'est la raison pour laquelle Internet et plus largement le cyberespace sont très tôt apparus comme un moyen d'accéder directement aux diverses audiences cibles recherchées par la mouvance. Dès la fin des années 1990 apparaissent les premiers sites Internet relayant l'idéologie radicale djihadiste et se faisant l'écho de l'actualité sur les différents fronts du djihad. Ainsi, au début 2000, al-Qaïda se dote de son propre site web, et lance sa propre agence de production audiovisuelle, As-Sahab. Celle-ci diffuse rapidement sa première vidéo en ligne, pour saluer l'opération-suicide contre l'*USS Cole*, qui aboutit à la mort de 17 marins américains le 12 octobre 2000[37]. Cependant, les grands sites liés à al-Qaïda s'avèrent très instables : ils pâtissent d'attaques et de procédures régulières de services gouvernementaux ou d'activistes. Les djihadistes apprennent néanmoins à contourner ces blocages, et se font une spécialité de la création de « sites miroirs », qui permettent de renforcer la résilience de la présence djihadiste sur Internet.

Au tournant des années 2000 cette première couche est complétée par la multiplication des « forums », arabophones ou non, sur lesquels les djihadistes peuvent échanger de façon moins centralisée, et faire vivre une « communauté de pratiques » mise à mal par la traque implacable à laquelle sont désormais soumis les cadres d'al-Qaïda. C'est également sur ces forums que sont publiés des ouvrages majeurs de théoriciens du djihad tels que la

37. G. Weimann, *Al Qa'ida's Extensive Use of the Internet*, CTC Sentinel, Westpoint, vol. 1, n° 2, 2018.

Gestion de la Sauvagerie d'Abou Bakr Naji vers 2004 ou l'*Appel à la résistance islamique mondiale* d'Abou Moussab al-Souri. Cette évolution vers le web participatif se traduit aussi par l'investissement précoce des réseaux sociaux. Dès 2008, un appel est ainsi lancé sur le forum djihadiste Al-Falloujah à « envahir » Facebook et YouTube, pour y animer des groupes favorables à al-Qaïda et y diffuser des vidéos de propagande[38]. Aidés par certains membres venus des États-Unis et sensibilisés avant les autres à l'enjeu des réseaux sociaux les groupes djihadistes Harakat al-Shebab en Somalie et al-Qaïda dans la péninsule arabique – surtout implanté au Yémen, se distingue par un activisme important sur YouTube et Facebook, et une production de contenus originaux rompant avec la monotonie des communiqués de la branche centrale d'al-Qaïda. Toutefois, beaucoup de djihadistes se montrent encore méfiants vis-à-vis des grands réseaux sociaux, créés aux États-Unis et soupçonnés par les radicaux d'être affiliés aux services de renseignement américains[39].

C'est au tournant de la décennie 2010 que le djihad médiatique atteint sa pleine mesure sur les réseaux sociaux dont s'empare alors la jeunesse moyen-orientale à l'occasion du Printemps arabe. Se fondant dans ce mouvement de masse, les djihadistes restent longtemps dans l'impunité, protégés par la « neutralité du Net » alors professée par les grandes plateformes californiennes, qui ne cachent pas leur sympathie envers le mouvement d'émancipation qui semble alors en cours. Ce faisant, les djihadistes atteignent une audience encore inégalée, d'une part parce qu'ils attisent les réactions de révolte, de victimisation et de désir de vengeance face à la répression du régime de Bachar al-Assad en Syrie, et d'autre part du fait de la viralité, des phénomènes d'amplification et de la « sérendipité » des algorithmes aiguillant le parcours des utilisateurs de réseaux sociaux.

À partir de 2012, le djihad syrien commence à attirer des centaines puis des milliers de jeunes adultes, voire d'adolescents, rompus à l'usage des réseaux sociaux. Les pages Facebook et les comptes Twitter de ces sympathisants gagnent en popularité, et des vedettes de la djihadosphère émergent. Twitter devient rapidement le principal vecteur de diffusion de liens vers des contenus djihadistes, notamment vers des vidéos de propagande sur YouTube. À la fin de l'année 2014, selon une étude de la RAND Corporation, l'EI disposait en 2014 d'un réseau de plus de 46 000 comptes utilisateurs sur Twitter, dont un noyau dur « hyperactif » (disposant de plusieurs milliers d'abonnés par compte) permettant aux

38. M. Hecker, « Web social et djihadisme : du diagnostic au remède », *Focus stratégique*, n° 57, Ifri, juin 2015.
39. *Ibid.*

contenus associés d'apparaître régulièrement parmi les *trending topics* de la plateforme[40].

Si la stratégie d'influence existe chez tous les groupes djihadistes, elle atteint une nouvelle dimension avec l'avènement de l'EI qui institutionnalise l'action dans le cyberespace, entre 2014 et 2015. Sous l'autorité du syrien Abou Mohammed al-Adnani, porte-parole de l'organisation, Daech parachève son appareil de cyber-influence, extrêmement structuré et efficace. Ses propagandistes sont recrutés parmi « d'anciens journalistes, vidéastes amateurs ou de bons connaisseurs des réseaux sociaux ». Comptant parmi les cadres les plus privilégiés de l'organisation – résidence de fonction, exemption d'impôts, salaires confortables – les « cyber-djihadistes » sont scrupuleusement formés et équipés de matériel de pointe[41]. De la publication de courts messages sur les réseaux sociaux à l'édition de webmagazines soignés, en passant par la diffusion de reportages de guerre filmés en GoPro et de « super-productions » à grand renfort d'effets spéciaux, l'EI déploie une gamme extrêmement variée de formats et de contenus, afin de toucher une audience toujours plus large. Au moment de la prise de Mossoul, l'EI est ainsi en mesure de diffuser 40 000 tweets en une seule journée[42].

Les structures de propagande de l'État islamique

L'organisation s'appuie à son apogée sur une structure centralisée, un bureau central des médias (*Diwan al-Ilam al-Markazi*) exerçant un contrôle direct et étroit sur au moins six « fondations médiatiques », segmentées en fonction des audiences cibles[43]. La fondation *al-Furqan*, créée dès 2006, dispose d'importants moyens pour produire des contenus arabophones, aussi bien écrits que visuels, pouvant aller de l'affiche de propagande au long-métrage mettant en scène les exploits guerriers des combattants du djihad. Elle peut également se prêter à des formats plus « journalistiques » et même à de la communication politique, comme lorsqu'en avril 2019, elle réalise un enregistrement vidéo du leader Abou Bakr al-Baghdadi, afin de démentir sa mort et de donner les lignes directrices de l'organisation. Créé en 2014, l'*al-Hayat Media Center*, dont le logo doré n'est pas sans rappeler celui d'Al Jazeera, s'est quant à lui spécialisé dans la production de contenus

40. E. Bodin-Baron *et al.*, *Examining ISIS Support and Opposition Networks on Twitter*, Santa Monica, RAND Corporation, 2016.
41. J.-F. Poisson et K. Arif, *Rapport d'information au nom de la mission parlementaire sur les moyens de Daech*, Paris, Assemblée nationale, n° 3964, 13 juillet 2016.
42. M. Hecker, « Web social et djihadisme : du diagnostic au remède », *op. cit.*
43. D. Milton, « Communication Breakdown: Unraveling the Islamic State's Media Efforts », Combating Terrorism Center at West Point, octobre 2016.

qu'il diffuse en langues étrangères, en particulier les webmagazines *Dabiq* en anglais ou *Dar al-Islam* en français. La même année qu'al-Hayat est créée « l'agence de presse » *Amaq*, confiée à un ex-reporter syrien opposé à Bachar al-Assad qui documentait les exactions du pouvoir avant de rejoindre Daech, et dont le ton apparemment « neutre » donne l'impression d'un organe médiatique indépendant[44]. L'organisation dispose également de sa propre radio,
al-Bayan, diffusant en diverses langues sur les bandes FM depuis des émetteurs situés à Raqqa et Mossoul – qui furent détruits en 2017. La station travaille en étroite collaboration avec la fondation *al-Ajnad*, spécialisée dans la production sonore, et tout particulièrement de *nashid*, chants masculins *a capela*, louant l'épopée des moudjahidines et qui sont l'un des produits phare de la propagande djihadiste, du fait de leur très importante viralité[45]. Enfin, une dernière agence, baptisée *Nashir*, s'est spécialisée dans la communication sur les chaînes de messagerie telles que Telegram.

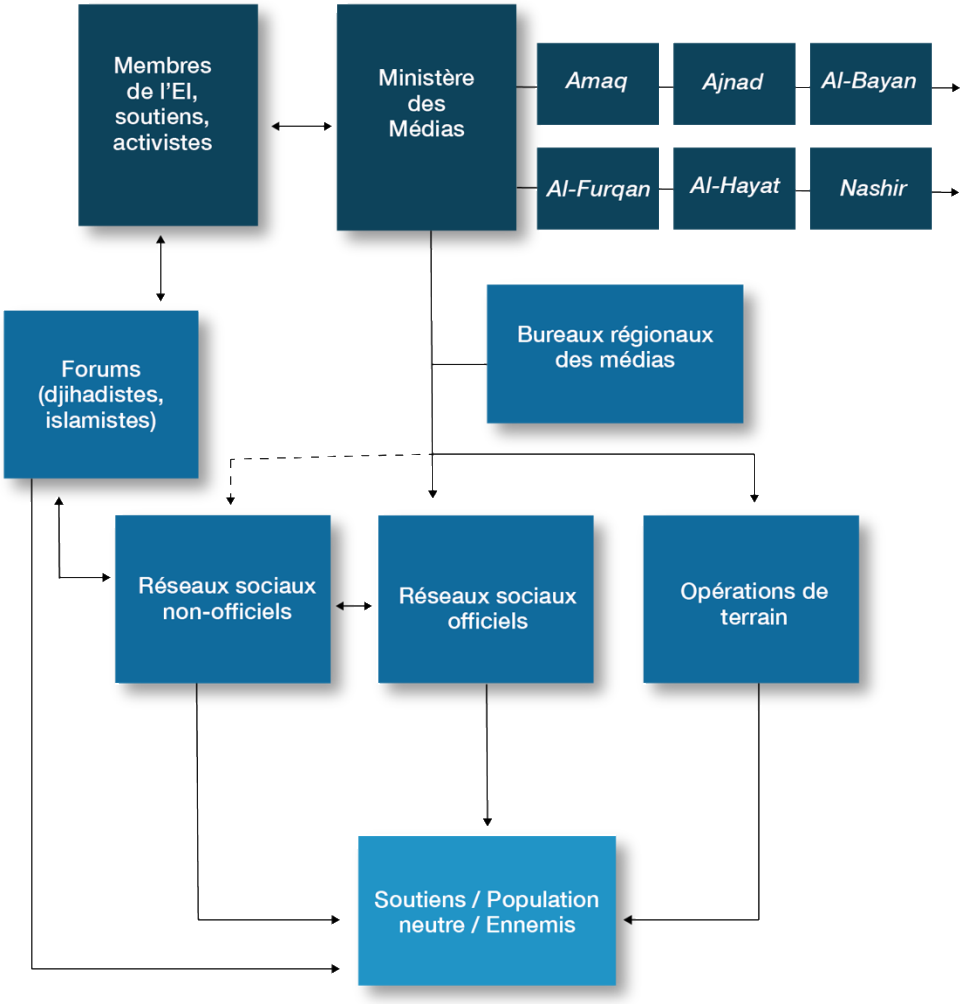
Outre l'activité centralisée de l'organisation, l'EI avait divisé son territoire en entités administratives (*wilaya*), dont chacune diffusait ses propres contenus en ligne sous le contrôle du *Diwan*, alimentant également sa banque d'information pour la production de futurs contenus[46]. La guerre informationnelle de Daech se déploie aussi en marge des structures « officielles » du groupe à travers un certain nombre d'officines telles qu'*Alhut-Tawhid*, qui disposait de serveurs en Arabie Saoudite et aux Émirats arabes unis (EAU). Cette galaxie de « sympathisants » n'apparaissant pas directement dans la chaîne de commandement informationnel de l'EI a joué un rôle important de relais des messages officiels, et de résilience de la propagande en ligne avec notamment la création de contenus propres, alors que les structures centrales sont mises à mal par les opérations de la coalition internationale, aussi bien dans les champs matériels et que cyber (*cf. infra*).

À partir de 2015 et de façon accélérée à partir de la chute des principales emprises territoriales de l'EI – Mossoul et Raqqa – en 2017, la cyber-propagande du « califat » a effectivement dû se réorganiser. Une partie des agences et fondations médiatiques ont été dissoutes ou restructurées et la production de contenu a souffert d'une chute incontestable dans son rythme et sa diffusion. Du fait de la suppression massive des contenus extrémistes sur les plateformes numériques, les djihadistes ont cherché des échappatoires, investissant massivement dans des applications chiffrées,

44. A. Almohammad et C. Winter, *Battlefront to Cyberspace*, CTC Westpoint, juin 2019.
45. H. Gråtrud, « Islamic State *Nasheeds* As Messaging Tools », *Studies in Conflict & Terrorism*, décembre 2016, vol. 39, nº 12, p. 1050-1070.
46. *The Virtual Califate: Understanding Islamic State's Propaganda Strategy,* Quilliam, juillet 2015.

tout en essayant régulièrement de refaire surface sur des plateformes grand public[47].

Schéma n° 2 : Architecture simplifiée de la cyber-influence de l'État islamique en 2015



Diffuser le message djihadiste

Dans un rapport intitulé *The Islamic State,* Richard Barrett, ancien chef du contre-terrorisme au MI5 souligne que la stratégie d'influence de l'EI « a su tirer le maximum de la nature décentralisée des réseaux sociaux, qui permet à chacun de ses supporteurs de créer et d'animer son propre ministère de l'information[48] ». De plus, comme l'explique le politologue Asiem El

47. M. Hecker et É. Tenenbaum, « Quel avenir pour le djihadisme ? Al-Qaïda et Daech après le califat », *Focus stratégique*, n° 87, Ifri, janvier 2019.
48. R. Barrett, *The Islamic State*, Soufan Group, 2014.

Difraoui, l'organisation a su tirer son épingle du jeu par une maîtrise des codes de la *pop culture*. Aux interminables prêches face caméras d'Ayman al-Zawahiri, leader d'al-Qaïda, les propagandistes du « califat » ont su opposer des vidéos spectaculaires, au montage trépidant, alternant des images brutes, parfois ultra-violentes, et des films travaillés, reprenant tous les codes des jeux vidéo de guerre, des émissions de télé-réalité et des *blockbusters* hollywoodiens[49]. Outre ces campagnes de cyber-propagande, somme toute assez classiques, la mouvance djihadiste a aussi démontré sa capacité à innover et à miser sur des formats plus originaux. Ainsi, en mars 2013, l'Institut de recherche des médias du Moyen-Orient a découvert sur le forum djihadiste Ansar al-Moudjahidine un jeu vidéo d'arcade intitulé « Le Mali musulman », dans lequel les joueurs étaient invités à détruire des avions de l'armée française ou à « mourir en martyr » dans le désert malien[50].

Parmi les techniques utilisées par l'EI pour diffuser massivement sa propagande sur les plateformes numériques, on peut citer le détournement de *hashtags* et le recours à des applications permettant de diffuser des contenus à très grandes échelles – telle que « Al Fajr al-basha'ir » qui permettait de transformer des sujets en *trending topics* sans déclencher les algorithmes de détection, et qui a été supprimée par Twitter en juin 2014. Par exemple, les *hashtags* #JustinBieber ou encore #WC2014 et #Brazil2014, très populaires pendant la coupe du monde de football de 2014, ont été détournés par des soutiens de l'EI pour diffuser des contenus djihadistes auprès d'un public plus large. Dans la même veine, les *hashtags* #stopdjihadisme, lancé par le gouvernement français à la suite des attentats de 2015, et #IwillcometoTunisia, apparu pour soutenir les Tunisiens après l'attaque du musée du Bardo, ont été largement détournés par des sympathisants de la mouvance.

Parmi les autres pratiques de cyber-propagande djihadiste, on trouve également des opérations informatiques offensives de bas niveau, n'exigeant pas de compétence avancée en matière de cyberattaques, comme le défacement de sites certains sites officiels gouvernementaux peu protégés, d'entreprises, de médias ou d'organisations. Ainsi, dans la semaine ayant suivi l'attentat contre Charlie Hebdo le 7 janvier 2015, 19 000 sites français ont fait l'objet de cyberattaques, très majoritairement peu sophistiquées[51]. Quelques jours plus tard en janvier 2015, un groupe se réclamant de Daech a piraté les comptes Twitter et Facebook du commandement militaire

49. C. Winkler et C. Dauber, *Visual Propaganda and Extremism in the Online Environment*, U.S. Army War College, Strategic Studies Institute, 2014.
50. « AQMI a conçu un jeu vidéo pour désintégrer l'armée française au Mali », *France 24*, 27 mars 2013, disponible sur : www.france24.com.
51. A. Ruello, « Vague de cyberattaques sans précédent en France », *Les Échos*, 15 janvier 2015.

américain au Moyen-Orient (CENTCOM). Tout comme dans l'attaque informatique contre TV5 Monde les 8 et 9 avril 2015, des doutes apparaissent rapidement sur l'origine réelle de l'attaque, bien plus complexe que les autres, une enquête diligentée par la Direction générale de la sécurité intérieure (DGSI) et mobilisant les experts de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) conduisant en réalité à pointer du doigt un groupe de hackers liés à la Russie[52].

Cette communication à outrance s'est avérée fort utile aux agences de renseignement, qui ont pu repérer des lieux d'entraînement et de vie des combattants. Toutefois, les djihadistes ont pris conscience des enjeux de sécurité opérationnelle, et la prudence a été recommandée sur les médias sociaux. Dès 2014, les sympathisants de l'EI ont été incités à moins communiquer sur les réseaux, à ne pas évoquer leurs activités sur les plateformes numériques, à ne pas s'afficher comme des membres de l'organisation, et à utiliser des alias. Occasionnellement, les organisations djihadistes ont même cherché à tourner à leur profit l'observation méticuleuse de leur activité en ligne par leurs adversaires en s'essayant à des formes rudimentaires de déception et d'intoxication[53]. Par exemple, lors des manifestations qui ont suivi la mort de Georges Floyd aux États-Unis au printemps 2020, plusieurs membres d'un forum en ligne de l'EI ont incité à infiltrer les conversations sur la tension raciale et à exacerber celles-ci en se faisant passer pour des Afro-Américains d'une part et des tenants de la suprématie blanche d'autre part, et en postant des messages incendiaires pour semer la zizanie[54].

Recruter des candidats au djihad

Avec le développement des filières djihadistes vers la Syrie, le recrutement sur Internet prend une nouvelle ampleur. Les réseaux sociaux, en particulier Facebook, deviennent le terrain de chasse de rabatteurs, qui, à la manière des chasseurs de têtes, repèrent les potentiels candidats au djihad – aussi bien pour les encourager à rejoindre la zone syro-irakienne et ainsi émigrer vers la terre d'islam (*hijira*) lorsque cette perspective existait, entre 2014 et 2017, que pour les inciter à conduire des attentats dans leur propre pays, ce qui semble le message privilégié depuis quelques années maintenant.

52. S. Leblal, « Piratage de TV5 Monde, la piste russe se précise », *Le Monde informatique*, 10 juin 2015.
53. C. Whiteside, « Lying to Win: The Islamic State Media Department's Role in Deception Efforts », *The RUSI Journal*, 2020; D. Milton, « Truth and Lies in the Caliphate: The Use of Deception in Islamic State Propaganda », *Media, War & Conflict*, 2020, p. 1-17.
54. L. Bindner, « Groupes djihadistes et mouvement de protestation aux États-Unis : réactions et tentatives d'instrumentalisation », *Ultima Ratio*, 29 juin 2020.

À son apogée, le succès du recrutement de l'État islamique s'explique par la conjonction de plusieurs facteurs. Tout d'abord les victoires militaires sur le terrain, en zone syro-irakienne, alimentent et soutiennent une mise en récit valorisant de la dynamique djihadiste. Ensuite, la professionnalisation des « équipes médias » permet la production de contenus attractifs, variant les thèmes et les formats. Aux images spectaculaires de combats filmés au ralenti s'ajoutent des formats plus proches du quotidien avec la reprise des codes de la télé-réalité et la mise en scène de la vie des combattants au « Sham » (Levant). Des vidéos montrent ainsi des journées ordinaires des moudjahidines, loin des combats, des moments de détente entre « frères », des distributions de nourriture, des travaux agricoles ou de construction de routes. Des photographies de certificats de naissance ou de plaques d'immatriculation frappés du sceau de l'EI ont également circulé sur les réseaux sociaux.

Enfin, la diffusion et l'amplification de ce message grâce à d'autres équipes dédiées sont le dernier facteur de succès conduisant à une viralité qui a longtemps bénéficié des algorithmes des plateformes, fonctionnant de telle manière que si un utilisateur s'intéressait à certains thèmes (le conflit en Syrie ou le salafisme par exemple), il se voyait suggérer de plus en plus de contenus liés à ces thématiques. En quelques jours, il pouvait voir son fil d'actualité rempli d'images de propagande djihadiste, et être contacté par des facilitateurs susceptibles de lui donner des indications précises sur la manière de rejoindre la Syrie[55]. Si ce mécanisme, parfois qualifié « d'enfermement algorithmique » a pu faire l'objet de rectification par les grands acteurs du web social, lesquels ont pris de forts engagements dans la lutte contre les discours de haine et « l'extrémisme violent », ils ont de fait pendant longtemps facilité – involontairement bien sûr – le travail des recruteurs du djihad.

Orientations stratégiques et instructions tactiques

Dans une tribune parue en novembre 2014 dans le *Financial Times*, Robert Hannigan, alors à la tête du Government Communications Headquarters (GCHQ) britannique prévenait qu'Internet était devenu pour l'organisation État islamique un véritable « centre de commandement et de contrôle[56] ». En effet, la mouvance djihadiste investit aussi le cyberespace pour diffuser des orientations stratégiques et des conseils tactiques. Cette évolution n'est pas récente. Les orientations stratégiques ont toujours fait partie intégrante

55. M. Hecker, « Web social et djihadisme : du diagnostic au remède », *op. cit.*
56. R. Hannigan, « The Web Is a Terrorist's Command-and-control Network of Choice », *Financial Times*, 3 novembre 2014.

de la propagande djihadiste, appelant à toutes les « bonnes volontés » pour lutter contre les adversaires désignés, et leur transmettant les lignes directrices, le positionnement, les perspectives, et les instructions du groupe. Sur le plan des instructions opérationnelles et tactiques, dès 2003, les partisans d'al-Qaïda en Arabie Saoudite avaient lancé un magazine en ligne intitulé *Camp Al-Battar* (*mu'askar al-battar*) dont l'ambition était d'être un véritable camp d'entraînement virtuel pour djihadistes. En 2011, le web magazine anglophone *Inspire* produit par al-Qaïda dans la péninsule arabique avait multiplié les instructions pratiques pour conduire des attentats, dont un article devenu célèbre et intitulé « Comment fabriquer une bombe dans la cuisine de votre maman[57] ».

L'État islamique s'est largement inscrit dans ce sillage avec la publication en 2015 d'un manuel intitulé *How to survive in the West: A Mujahid Guide* dans lequel se trouvent des instructions techniques sur la manière de préserver son anonymat sur le web *via* des réseaux privés virtuels (VPN) ou des clés de chiffrement. Mais le document offrait aussi de recommandations pratiques et opérationnelles dans le champ matériel : comment acheter des armes, fabriquer des explosifs ou encore employer un véhicule-bélier[58]. Ces procédures destinées à permettre à l'opérateur d'agir en autonomie relative, ont parfois été complétées par un suivi plus personnalisé *via* des chaînes de communication sécurisées, donnant ainsi lieu à une forme de « terrorisme téléguidé ». Telegram en particulier, est devenu l'outil de communication préféré des membres de l'EI, non seulement pour peaufiner le recrutement de volontaires, mais aussi pour coordonner différentes cellules dans le cadre d'un attentat ou d'une attaque[59].

La mouvance djihadiste utilise enfin le cyberespace pour lever des fonds, que ce soit pour subventionner les départs vers le « Sham » ou financer des attaques sur le territoire européen. Un jugement de 2011 a par exemple permis d'établir que certains forums djihadistes, tel que Minbar-SOS, n'étaient pas que de simples lieux de discussions. Les échanges d'argent entre plusieurs participants ont en effet permis de financer des voyages d'Europe occidentale vers le Waziristan. Parmi les techniques de levée de fonds utilisées par la mouvance djihadiste, on peut également citer le *crowdfunding* (financement participatif) *via* l'usage de crypto-monnaies, et les arnaques en tous genres sur le web (sur les sites de rencontre par exemple)[60].

57. « Make a Bomb in the Kitchen of Your Mom », *Inspire*, n° 1, été 2010, p. 33-40.
58. « Just Terror Tactics », *Rumiyah*, n° 3, safar 1438, p. 10-12.
59. M. Bloom, H. Tiflati et J. Horgan, « Navigating ISIS's Preferred Platform: Telegram », *Terrorism and Political* Violence, vol. 31, n° 6, 2019.
60. S. Diffalah, « Financement du terrorisme : le crowdfunding en ligne de mire », *L'Obs*, 20 avril 2015.

Si aujourd'hui la force de frappe de la cyber-influence djihadiste a considérablement réduit, il faut toutefois garder à l'esprit les caractéristiques de la présence sur les réseaux sociaux des mouvements djihadistes : la flexibilité, la vitesse et la résilience[61]. Le chercheur Ali Fisher compare d'ailleurs cette présence à une nuée d'oiseaux se dispersant momentanément, avant de se reformer sitôt que la menace est passée. Les grandes opérations de « nettoyage » des plateformes organisées par les services gouvernementaux et les hébergeurs – à l'instar de celle lancée en novembre 2019 sur Telegram[62] – ont affaibli la capacité de cyber-influence djihadiste sans l'anéantir pour autant.

La production de contenus n'a pas cessé, même si elle a réduit en fréquence et parfois en qualité. Sa diffusion, quoique globalement confinée à des plateformes plus confidentielles tente régulièrement de faire des retours fugaces sur le web « mainstream ». Cette ambition se traduit par des manœuvres de harcèlement et des démonstrations de forces, par exemple avec liens multiples et des *hashtags* de ralliement, ainsi que par une pression accrue sur les réseaux sociaux. Ainsi, en novembre 2020, plusieurs médias francophones dont *Le Monde* ont fait l'objet d'une campagne de propagande djihadiste coordonnée sur Facebook, au cours de laquelle plus de 700 messages empruntant au corpus de l'EI ont été diffusés en quelques minutes[63].

La mouvance djihadiste a par ailleurs pleinement tiré profit des fonctionnalités éphémères de type « stories » ainsi que d'une forte mobilité d'une plateforme à l'autre en fonction des régulations qu'elles mettent en œuvre : après Telegram, les grands diffuseurs de contenus djihadistes ont ainsi migré vers Tamtam, puis Hoop, Rocketchat et Élément (anciennement Riot.im) utilisant le protocole Matrix, décentralisé et chiffré de bout en bout y compris dans les « salons » (*chatrooms*). Pour survivre et éviter la répression, la mouvance multiplie aussi les « faux-nez » et les chaînes non officielles se faisant passer pour de simples sympathisants islamistes, moins exposés aux mesures d'interdiction et à l'action des modérateurs en ligne.

États-Unis : la grande convergence cyber-informationnelle

Aux États-Unis, la prise en compte des enjeux informationnels et de l'influence militaire en général, et dans le cyberespace en particulier, est

61. Cité dans M. Hecker, « Web social et djihadisme : du diagnostic au remède », *op. cit.*
62. L. Bindner, R. Gluck, « Affaiblie mais pas hors jeu : les récentes mutations de la propagande de l'EI », *Ultima Ratio*, 27 janvier 2020.
63. M. Untersinger, « Une campagne de propagande djihadiste coordonnée sur les pages Facebook de médias français », *Le Monde*, 24 novembre 2020.

ancienne, et a fait l'objet de nombreux travaux. Elle renvoie toutefois à une évolution constante des définitions et des acteurs impliqués. La notion même de lutte informationnelle (*information warfare*) a longtemps souffert d'une très forte polarisation entre d'une part les branches techniques issues de la guerre électronique, du renseignement technique (SIGINT) et de la lutte informatique (*cyberspace operations*) et d'autre part les acteurs issus du champ sémantique, de la communication stratégique et des opérations d'information.

Alors que la dimension technique de la guerre de l'information a très tôt reçu un appui prioritaire dans le cadre des grands projets de révolution dans les affaires militaires (RMA), comme *Transformation* ou la *Third Offset Strategy*, la dimension sémantique et cognitive est demeurée une préoccupation plus minoritaire, aussi bien au sein de l'institution militaire que dans la diplomatie. La sensibilité politique autour des notions de propagande ou de désinformation a été démontrée à plusieurs reprises, comme dans le cas de l'Office of Strategic Influence créé en 2002 par Donald Rumsfeld et aussitôt démantelé après que la presse a révélé qu'il envisageait le recours à l'intoxication.

L'architecture de cyber-influence américaine

Les États-Unis sont les premiers à avoir adopté le terme de « communication stratégique » comme principe intégrateur inter-agences sous la houlette de la Maison-Blanche et du National Security Council[64]. C'est toutefois le Département d'État qui a été identifié comme l'agence cadre pour conduire la communication stratégique à travers son Sous-Secrétaire d'État à la diplomatie publique. Sous son autorité se trouve le Global Engagement Center (GEC) créé en 2016 après le vote par le Congrès du *Countering Foreign Propaganda and Disinformation Act*. Le GEC a notamment pour mission de coordonner les efforts du gouvernement pour lutter contre la propagande et la désinformation d'acteurs étrangers[65].

Le Département de la Défense se positionne en second rideau de la communication stratégique et de la manœuvre d'influence globale. Il se concentre sur l'appui informationnel aux forces et opérations militaires. En l'attente d'une nomination d'un *Principal Information Officer* directement rattaché au Secrétaire à la Défense, c'est l'*Assistant Secretary* pour les opérations spéciales et les conflits de faible intensité (ASD SO/LIC) qui a la

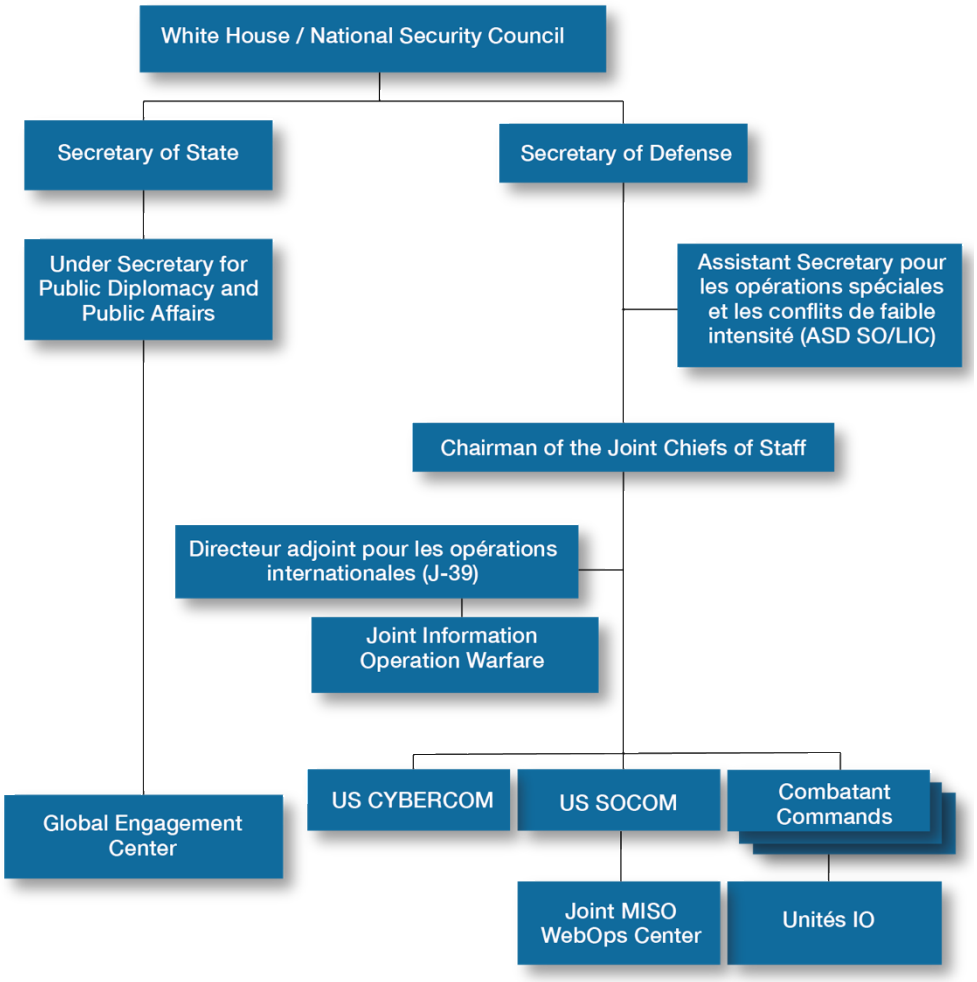
64. *U.S. National Strategy for Public Diplomacy and Strategic Communication*, State Department, juin 2007.
65. C. A. Theohary, *Defense Primer: Information Operations*, Washington, DC, Congressional Research Service, décembre 2020.

responsabilité politique de superviser toutes les opérations d'information, qu'elles soient numériques ou non. À l'échelon militaire, c'est le directeur adjoint pour les opérations internationales (J-39), placé sous l'autorité du chef d'état-major des armées (*Chairman of the Joint Chiefs of Staff*) qui veille à la coordination opérationnelle, notamment par le biais du Joint Information Operations Warfare Center. Ce dernier a pour tâche de mettre en cohérence les différentes capacités informationnelles opérationnelles.

Au niveau opérationnel, les capacités en question se répartissent entre d'une part les commandements des opérations spéciales (SOCOM) et du cyber (CYBERCOM) et d'autre part les commandements combattants régionaux (*European Command, Central Command, Indopacific Command*, etc.). Ce sont ces derniers qui disposent en règle générale du contrôle opérationnel sur les unités opérationnelles de guerre de l'information, y compris dans le cyberespace, ce dont le *Central Command* a été précurseur. C'est toutefois le SOCOM qui conserve la prérogative organique en matière de *Military Information Support Operations* (MISO) – la mission recouvrant la plupart des activités d'influence – et vient en appui des commandements régionaux. Il a pour ce faire mis en place un centre pour les opérations web (*Joint MISO Web Ops Center*) lequel assure, avec ses quelque 250 personnels – un chiffre qui devrait tripler d'ici 2025 – la publication de contenu et la veille des activités des adversaires sur les réseaux sociaux. C'est également le *Web Ops Center* de SOCOM qui assure la liaison et la coordination opérationnelle avec certains pays alliés[66]. Dans le même ordre d'idée, le CYBERCOM a mis sur pied la *Cyber Mission Force* qui, si elle gère les opérations de lutte informatique au niveau national, opère surtout en appui des commandements régionaux. Dès lors que l'opération envisagée implique la mobilisation de capacités de lutte informatique offensive, le CYBERCOM récupère le contrôle opérationnel de ses *Cyber Combat Mission Teams,* dont l'action doit rester « alignée » sur les objectifs du commandement impliqué.

66. Entretien avec un officier du ministère des Armées.

Schéma n° 3 : Architecture simplifiée de la cyber-influence aux États-Unis



Produire et diffuser un contre-discours

Le premier volet de l'influence américaine dans le cyberespace tient à la production et à la diffusion de contenus en ligne. Ainsi, le Center for Strategic Counterterrorism Communications (CSCC), ancienne unité du département d'État créée en 2011, était chargée de produire un récit américain unifié et calibré pour contrer les idéologies extrémistes sur Internet. Il était doté d'une *Digital Outreach Team* chargée de la sensibilisation numérique, dont la campagne la plus marquante « *Think Again Turn Away* » a été lancée en décembre 2013. Elle a fait interagir directement des combattants de l'EI avec des membres de l'unité. Cependant, tous les contenus produits par la *Digital Outreach Team* étaient estampillés du département d'État, ce qui les a empêchés d'atteindre un

certain nombre de militants islamistes extrémistes et a fortement réduit leur diffusion[67].

C'est pour remédier à ce problème qu'a été créé en 2016 le *Global Engagement Center*. Celui-ci s'est associé au *Sawab Center* des EAU dans le cadre de sa lutte contre la propagande de l'État islamique au sein du monde arabophone. Les campagnes de contre-discours en ligne du *Sawab Center* se sont avérées nettement plus efficaces que celles du CSCC, parce qu'elles n'étaient pas directement affiliées aux États-Unis. La campagne « *deludedfollower* » par exemple, qui abordait la question des combattants étrangers, a enregistré 163 millions d'impressions sur Twitter[68]. L'association avec des acteurs locaux est donc une piste prometteuse pour élaborer et diffuser efficacement un contre-discours sur les plateformes numériques.

En parallèle de cette campagne conduite par le département d'État, le *Web Ops Center* du CENTCOM a mis sur pied de son côté un service de *Online Persona Management*, qui gère des avatars en ligne dans le monde entier. Chaque employé de ce service est responsable d'une dizaine de *persona* en ligne, qui propagent des narratifs favorables aux intérêts des États-Unis et s'opposent aux propos hostiles[69]. Le CENTCOM a ainsi été à l'origine de l'opération *Earnest Voice*, qui visait à contrer l'influence des organisations islamistes en Irak, en Afghanistan et au Pakistan. En achetant à la firme Ntrepid une solution spécifique aux forums en langues locales (arabe, farsi, ourdou et pachtoune), le CENTCOM a pu créer de nombreux avatars sur les plateformes ciblées, et ainsi dresser une cartographie des principaux acteurs. Ensuite, ces faux comptes ont été utilisés pour diffuser de la propagande pro-américaine et contrer les narratifs adverses[70].

Perturber les activités en ligne de l'adversaire

À l'automne 2016, dans le cadre la coalition internationale contre l'État islamique, les États-Unis ont lancé l'opération *Glowing Symphony* conduite sous l'égide de CENTCOM avec l'appui du SOCOM, du CYBERCOM et de la NSA. Cette opération visait à semer la confusion et à influencer les perceptions des combattants de l'EI, pour amoindrir leur efficacité

67. A. Reed, H. Ingram et J. Whittaker, *Countering Terrorist Narratives*, Bruxelles, Commission des libertés civiles, de la justice et des affaires intérieures, Parlement européen, 2017.
68. *Ibid.*
69. K. J. Boyte, « An Analysis of the Social-Media Technology, Tactics, and Narratives Used to Control Perception in the Propaganda War Over Ukraine », *Journal of Information Warfare*, vol. 16, n° 1, mai 2017, p. 88-110.
70. I. Cobain, « Revealed: US Spy Operation That Manipulates Social Media », *The Guardian*, 17 mars 2011.

opérationnelle et perturber leurs activités en ligne. Elle a débuté par la compromission du système d'information et du réseau des djihadistes grâce à une campagne d'hameçonnage (*phishing*) qui a permis de cartographier leur environnement informatique. À partir de cette cartographie, des *patterns* ont été identifiés (manière de nommer leurs comptes sur les réseaux, horaires de fréquentation des sites, plateformes privilégiées, etc.). Des informations détournées ont ensuite été introduites dans leur écosystème pour compromettre leurs activités. Ces dysfonctionnements ont perturbé les activités en ligne des combattants, en particulier la propagande, le recrutement, la communication et les levées de fonds. Finalement, la totalité des serveurs adverses a été détruite[71]. L'un des responsables de l'opération attribue par ailleurs les retards et les irrégularités de publications puis la cessation du web magazine *Rumiyah* à cette opération, ainsi que la suppression de 40 % puis 90 % des sites Internet de Daech.

On observe ici l'articulation de moyens de lutte informatique offensive et de lutte informationnelle dans le cyberespace pour déstabiliser au maximum l'adversaire. L'objectif assumé de ces opérations est de contrer les tentatives de délégitimation sur les plateformes des opérations extérieures des États-Unis et de leurs alliés. L'intégration et la synchronisation des capacités cyber sont ainsi exploitées pour produire des effets informationnels utiles sur le plan opérationnel, afin de réaliser des objectifs militaires. La révélation de cette opération s'inscrit enfin dans une stratégie de communication plus offensive autour des capacités de cyber-influence américaines. Il s'agit à la fois de rassurer les citoyens américains et de dissuader les adversaires par la démonstration de leur expertise, notamment en vue des élections présidentielles de novembre 2020.

71. D. Temple-Raston, « How the U.S. Hacked ISIS », *NPR*, 26 septembre 2019.

Coopérer avec le secteur privé

L'une des forces des États-Unis tient à ce que leur stratégie d'influence puise ses ressources au-delà du seul cercle des acteurs publics officiels. Selon Tim Maurer, auteur d'un ouvrage sur les « cyber-mercenaires », il existe trois types de relations de sous-traitance : la délégation, l'orchestration et la sanction (approbation ou autorisation). La délégation renvoie à une relation étroite sous le contrôle effectif de l'État. L'orchestration s'applique aux sous-traitants disposant d'une marge de manœuvre plus importante, par exemple s'ils reçoivent des fonds ou des outils mais pas d'instructions spécifiques. La sanction, enfin, se fonde sur le partage de valeurs communes ou une convergence d'intérêts partagés plutôt que sur un contrat[72].

Les *contractors* engagés par le Pentagone se trouvent majoritairement dans une situation de délégation. En effet, l'appareil de défense américain a externalisé une partie de ses activités de lutte informationnelle dans le cyberespace. À l'image de la collaboration du CENTCOM avec la firme Ntrepid lors de l'opération *Earnest Voice*, le CYBERCOM sous-traite certaines de ses activités à des acteurs privés. Ainsi, en 2016, il a noué un contrat de 460 millions de dollars sur cinq ans avec six compagnies pour soutenir ses missions[73].

- La première est la CACI, une entreprise fondée en 1960 par un ex-employé de la RAND. Basée à Arlington, en Virginie, elle emploie 20 000 personnes, et génère un chiffre d'affaires de 5,7 milliards de dollars. Elle se targue sur son site Internet de soutenir tous types d'opérations pour le compte du département de la Défense : « le personnel analyse les systèmes, les réseaux et les plateformes pour faciliter le cyber-ciblage dans le but d'identifier et de pénétrer les environnements cibles, des centres de données aux plateformes[74] ».
- La Science Applications International Corporation (SAIC) emploie 15 000 salariés et bénéficie de 4,3 milliards de dollars de revenus. Elle est engagée dans l'appui au Département de la Défense dans les questions d'influence depuis au moins les années 1990, et a joué un rôle clé pour mettre sur pied les stratégies médiatiques en Afghanistan et en Irak. Si l'on en croit ses offres d'emploi, elle emploie des planificateurs opérationnels dans le cyberspace, afin de mettre en œuvre les « plans, processus, procédures et directives gouvernementales en matière d'opérations offensives et

72. T. Maurer, *Cyber Mercenaries: The State, Hackers, and Power, op. cit.*
73. « CACI Wins Position on $460M Contract for US Cyber Command », *Army Technology*, 25 juillet 2016, article disponible sur : www.army-technology.com.
74. Site internet de la CACI, disponible sur : www.caci.com.

défensives dans le cyberespace[75] ».

- Les sociétés Booz Allen Hamilton, KeyW, Secure Mission Solutions, et Vencore comptent également parmi les six bénéficiaires de ce contrat avec le CYBERCOM. À ce titre, elles fournissent un support dans des domaines divers allant du défensif à l'offensif, en passant par l'administratif. En ce qui concerne Booz Allen Hamilton, il est probable qu'elle soit également impliquée dans des aspects offensifs[76]. C'est en effet l'une des plus grandes entreprises de la Base industrielle et technologique de défense (BITD) américaine, qui dispose de contrats tant avec les armées qu'avec les agences de renseignement. De plus, son département dédié au cyber a été développé par John M. McConnell, ancien directeur de la NSA et *Second Director of National Intelligence* entre 2007 et 2009[77].
- Dans la même veine, le gouvernement américain s'est plusieurs fois appuyé sur l'entreprise CrowdStrike, fondée en 2011 et connue notamment pour avoir enquêté sur les hackeurs russes responsables du piratage du DNC en 2016[78]. Entre 2015 et 2019, la société COLSA était quant à elle un sous-traitant du *WebOps Center* de SOCOM, à qui elle a fourni une suite logicielle permettant d'engager massivement sur les réseaux sociaux[79]. General Dynamics, une autre des principales entreprises de la BITD américaine, est arrivée plus récemment sur ce marché et a récupéré une majorité des parts de COLSA.

Russie : une cyber-influence agressive et clandestine

La Russie a ouvertement annoncé son ambition de leadership mondial en matière d'influence et de guerre de l'information, notamment dans le cyberespace où ses efforts convergent avec un investissement majeur dans le champ des capacités techniques et la recherche en IA[80]. L'approche russe est marquée par la conviction profonde de la menace incarnée par les démocraties libérales occidentales sur la pérennité de son régime. Les « révolutions de couleur » des années 2000, le Printemps arabe de 2011 ou la révolution ukrainienne de 2014 sont ainsi envisagés comme le résultat

75. Site internet de la SAIC, disponible sur : www.saic.com.
76. T. Maurer, *Cyber Mercenaries: The State, Hackers, and Power*, *op. cit.*
77. *Ibid.*
78. A. Au-Yeung, « What We Know About CrowdStrike: The Cybersecurity Firm Trump Mentioned in Ukraine Call, and Its Billionaire CEO », *Forbes*, 25 septembre 2019.
79. D. Butler et R. Lardner, « U.S. Military Botches Online Fight against Islamic State », *Chicago Tribune*, 31 janvier 2017.
80. « Concept de politique étrangère de la Fédération de Russie », Ministère des Affaires étrangères de la Fédération de Russie, 30 novembre 2016.

de vastes opérations d'influence orchestrées par les puissances occidentales contre des régimes jusqu'alors favorables.

Dans cette perspective, les campagnes d'influence et de déstabilisation dont on l'accuse ne sont présentées dans le narratif du Kremlin que comme la juste réponse défensive à des actions occidentales. Parmi les épisodes les plus marquants de cette campagne de propagande et de désinformation se trouvent l'ingérence dans les élections présidentielles américaines (2016) et françaises (2017) ainsi que les référendums sur le Brexit (2016) et l'indépendance de la Catalogne (2017). En effet, la Russie cherche en priorité à exploiter les clivages internes aux démocraties occidentales, tentant d'éroder la confiance des populations envers le modèle libéral et d'exacerber les fractures sociales.

Les acteurs de la cyber-influence russe

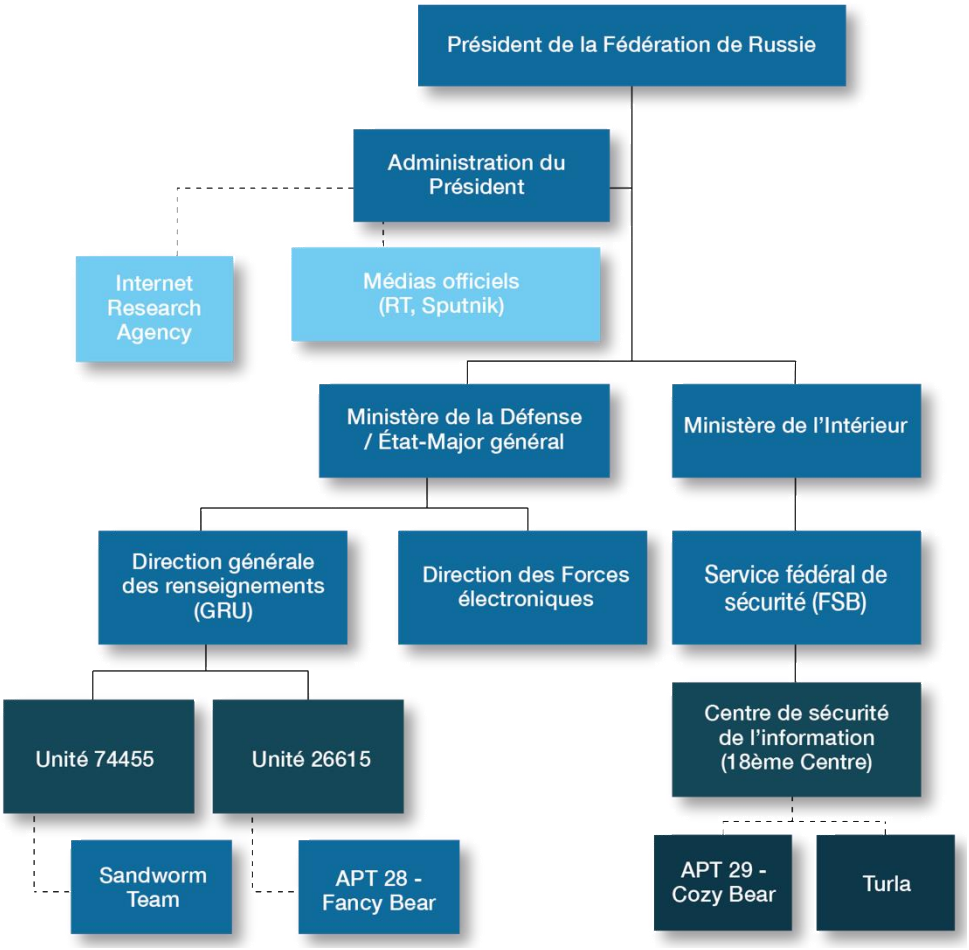
Pour ce faire, Moscou a adopté une approche intégrale et intégrée de la guerre de l'information, qui n'est pas marquée par la même bipolarisation que du côté occidental entre lutte informatique et électronique (technique) et stratégie d'influence. Cette différence tient principalement aux formes plus informelles de coordination que le Kremlin entretient entre les mondes politiques, militaires, civils et clandestins. En effet, sont inclus, aux côtés des moyens militaires et des services de renseignement, un certain nombre d'acteurs « civils » alignés sur les objectifs informationnels du pouvoir, au premier rang desquels les organes médiatiques Russia Today et Sputnik, disponibles dans plusieurs langues (anglais, français, arabe, et espagnol, notamment[81]). Intimement liés par des relations interpersonnelles à l'administration du président au Kremlin, ces derniers peuvent initier, ou servir de caisses de résonance pour des campagnes d'influence susceptible de s'insérer dans des schémas plus larges de déstabilisation[82].

Dans ce schéma, le ministère de la Défense et des Forces armées occupe néanmoins une place importante[83]. En 2017, les Forces armées de la Fédération de Russie ont officiellement annoncé la création de leur première unité de cyberdéfense, les « troupes d'opérations d'information », dont certains estiment qu'elles assurent des missions de contre-propagande en

81. S. Blank, « Cyber War and Information War à la Russe », *in* G. Perkovich, A. E. Levite, *Understanding Cyber Conflict: Fourteen Analogies*, Washington, DC, Georgetown University Press, novembre 2017.
82. S'ils ne sont pas sous l'autorité officielle du Kremlin, des liens personnels très forts existent entre Vladimir Poutine et Mikhaïl Lessine et Alexeï Gromov, les fondateurs des deux chaînes, qui ont d'ailleurs appuyé la nomination de Margarita Simonian, l'actuelle rédactrice en chef de RT et Sputnik. Voir M. Audinet, « Comment RT et Sputnik tissent la toile de Moscou à l'étranger », *La revue des médias*, INA, 19 juin 2019.
83. B. Tashev, M. Purcell et B. Laughlin, « Russia's Information Warfare: Exploring the Cognitive Dimension », *MCU Journal*, vol. 10, automne 2019.

ligne[84]. Ces troupes, dont le commandement de rattachement n'est pas clair, coordonnent et intègrent les cyber-opérations menées par les unités des forces armées russes, examinent le cyber-potentiel du ministère russe de la Défense et élargissent les possibilités de ses actions dans le cyberespace.

Schéma n° 4 : Architecture simplifiée de la cyber-influence en Russie



Toutefois, il apparaît que les principales cyber-capacités militaires russes dépendent de la Direction générale des renseignements (GRU). Cette dernière disposerait, au sein de sa direction du renseignement d'origine électromagnétique, de deux unités opérationnelles : 26165 et 74455, toutes deux spécialisées dans les attaques techniques. Aux côtés du GRU, l'autre acteur majeur des campagnes d'influence est le Service fédéral de sécurité (FSB) du ministère de l'Intérieur, qui dispose d'un Centre de sécurité de

84. M. Latsinskaya, A. Bratersky et I. Kalinin, « Россия ввела войска в интернет » [« La Russie a introduit des troupes sur Internet »], *Gazeta*, 22 février 2017, disponible sur : www.gazeta.ru.

l'information (Centre 18) dédié à la lutte informatique aussi bien sur le plan technique qu'informationnel[85].

Les groupes de pirates informatiques

Tout comme les États-Unis ont externalisé une partie de leur activité de lutte informationnelle dans le cyberespace, la stratégie d'influence russe puise des ressources au-delà du seul cercle des acteurs publics officiels. En juin 2017, le président Vladimir Poutine reconnaissait ainsi la possibilité que des « hackeurs patriotiques[86] » russes puissent avoir monté des cyberattaques en faveur d'intérêts russes à l'étranger. Les experts de la cybersécurité, privés aussi bien que gouvernementaux, ont depuis de nombreuses années déjà identifié des groupes de hackeurs travaillant sur des claviers en cyrillique, suivant les tranches horaires de la région de Moscou et opérant contre des cibles susceptibles de nuire aux intérêts du Kremlin.

Le premier groupe est connu sous le nom de *Fancy Bear* et désigné par l'opérateur de cybersécurité américain Mandiant comme la menace persistante avancée (*Advanced Persistant Threat,* APT) n° 28. Le groupe serait impliqué dans un grand nombre d'attaques telles que celle de TV5 Monde, déjà évoquée, ou les MacronLeaks de 2017. Le procureur Robert Mueller, en charge de l'enquête sur l'interférence russe dans les élections américaines de 2016, a formellement identifié *Fancy Bear* comme étant à l'origine du vol de données de la Convention nationale démocrate américaine[87]. Étroitement associé à *Fancy Bear*, le groupe de hackeurs *Sandworm Team* est lui aussi directement impliqué dans l'affaire des « DNC Leaks » – dans laquelle il s'est consacré à la diffusion des documents volés par *Fancy Bear* et à l'amplification de leur résonance – de même que dans plusieurs attaques dont celle contre le réseau électrique ukrainien en 2017. Toujours selon l'enquête Mueller, *Sandworm Team* serait en réalité lié à l'unité 74455 du GRU, et *Fancy Bear*, à l'unité 26615. Le Centre 18 du FSB est lui aussi associé avec des groupes de hackeurs bien connus, notamment le célèbre groupe *Cozy Bear* (APT 29) ou encore le groupe *Turla*.

Particulièrement compétents dans leurs opérations, ces acteurs se spécialisent sur les actions techniques d'intrusion, d'extraction de données, de sabotage par *malware*, etc., mais ces dernières peuvent participer à un

85. Q. Jurecic, « Government Indicts FSB Officers and Two Others in Yahoo Hacking Case », *Lawfare*, 15 mars 2017, disponible sur : www.lawfareblog.com.
86. « Patriotic Russians May Have Staged Cyber Attacks on Own Initiative – Putin », *Reuters*, 1er juin 2017.
87. R. S. Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election, op. cit.*

plan plus large visant à des actions d'influence dans le cyberespace[88]. D'autres groupes dits « hacktivistes » se concentrent davantage sur des activités de manipulation de l'information. Ainsi, entre mars 2017 et août 2020, des hackers russes ont mené une campagne de désinformation massive, surnommée *Ghostwriter*, dont l'objectif était vraisemblablement de discréditer l'OTAN et la présence américaine en Pologne et dans les États baltes. Pour ce faire, les hackers ont piraté les systèmes de gestion de différents sites d'information pour y diffuser de fausses informations, au sujet par exemple d'agressions perpétrées par des militaires américains, ou d'un plan d'invasion de la Biélorussie par l'OTAN[89].

Certains hacktivistes aident ainsi le gouvernement russe à diffuser ses narratifs et à déstabiliser ses adversaires. Lors de l'élection présidentielle ukrainienne de 2014, le groupe de hackers *CyberBerkut* s'est par exemple introduit dans le réseau central des élections, dont il a défacé le site Internet en faisant passer le candidat d'extrême droite pour le vainqueur de l'élection, alors qu'il n'avait recueilli que 0,7 % des voix[90]. Le défacement n'a été détecté qu'une heure avant l'annonce officielle des résultats du suffrage. Dans la même veine, des attaques DDoS ont été utilisées en 2008 pour soutenir l'engagement militaire russe en Ossétie du Sud : les sites du Parlement et de la présidence ont été défacés, et remplacés par des contenus comparant le gouvernement géorgien au régime nazi[91].

De la même manière, en avril 2020, le site Internet de l'Académie des arts et sciences polonaise a été piraté et défacé par des acteurs russes (encore non identifiés). Une fausse tribune du directeur de l'Académie incitant les soldats polonais à « lutter contre l'occupation américaine » a été diffusée et amplifiée par mail vers des cadres militaires de l'OTAN, mais aussi dans les médias polonais et sur les réseaux sociaux. Cette campagne visait à attiser un sentiment antiaméricain au sein de la population polonaise, et à saper le moral des troupes polonaises et américaines en Pologne, afin de tendre les relations du pays avec l'OTAN[92].

88. E. Bodine-Baron, R. C. Helmus, A. Radin, E. Treyger, *Countering Russian Social Media Influence*, Santa Monica, CA, RAND Corporation, 2018.
89. *"Ghostwriter" Influence Campaign: Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narratives Aligned with Russian Security Interests*, FireEye, 2020.
90. DGRIS, Observatoire du monde cybernétique, *Lettre mensuelle,* n°12, février 2020.
91. M. A. Miniats, *War of Nerves: Russia's Use of Cyber Warfare in Estonia, Georgia and Ukraine*, Senior Projects, Bard, Printemps 2019.
92. « Disinformation Attack on Poland », Site du gouvernement (Pologne), 23 avril 2020.

Les « usines à trolls »

L'idée d'enrôler des « trolls » favorables au Kremlin, qui puissent se faire les relais du discours officiel sur les réseaux sociaux, semble avoir émergé lors de l'hiver 2011-2012 face au mouvement de contestation des élections législatives russes alors qualifié par certains observateurs de « Révolution blanche ». Adoptant le modèle du Printemps arabe, ses organisateurs communiquaient massivement sur les réseaux sociaux, en particulier *Vkontakte* (l'équivalent russe de Facebook, fondé par Pavel Dourov, également créateur de la célèbre messagerie cryptée Telegram). En réaction, de nombreux soutiens au parti de Vladimir Poutine sont soudainement apparus sur ces plateformes, afin de créer des polémiques, semer la confusion et finalement affaiblir les opposants. Dès le retour à la présidence de Vladimir Poutine au printemps 2012, la reprise en main de web russe ne fait aucun doute, du rachat de *Vkontakte* par un groupe mieux contrôlé par le Kremlin au développement de l'activisme en ligne des « Nachi », un mouvement de jeunes nationalistes soutenant le président[93].

Tout comme les « hackeurs patriotiques », ces néo-trolls pro-gouvernementaux n'ont rien d'un mouvement spontané mais sont pour partie des employés d'entreprises privées entièrement dédiées à la lutte informationnelle dans le cyberespace. C'est tout particulièrement le cas de l'Internet Research Agency (IRA), la plus célèbre « fabrique à trolls » russe, basée à Saint-Pétersbourg. L'entreprise semble avoir été fondée en 2013 par l'oligarque Evgueni Prigojine, un proche du président ayant fait fortune en nouant de nombreux contrats avec le ministère de la Défense russe à travers sa compagnie Concord – il serait également le principal financeur de la société militaire privée Wagner[94]. Selon différentes sources l'IRA employait à la fin de la décennie plusieurs centaines de salariés aux profils variés : informaticiens, journalistes, bloggeurs, communicants, etc.[95]

L'entreprise s'est faite une spécialité d'inonder les fils d'actualité de propagande et de fausses informations, qui aident à promouvoir et amplifier les narratifs du Kremlin auprès d'audiences russes et étrangères[96]. Lors des élections américaines de 2016, l'IRA aurait mobilisé plus de 4 000 comptes humains et 50 000 *bots*, dont il est estimé qu'ils ont atteint une audience de

93. M. Elder, « Polishing Putin: Hacked Emails Suggest Dirty Tricks by Russian Youth Groups », *The Guardian*, 7 février 2012.
94. C. Gérard, « Usines à trolls russe : de l'association patriotique locale à l'entreprise globale », *La revue des médias*, INA, 20 juin 2019.
95. B. Popken et K. Cobiella, « Russian Troll Describes Work in the Infamous Misinformation Factory », *NBC News*, 16 novembre 2017.
96. E. Bodine-Baron, R. C. Helmus, A. Radin, E. Treyger, *Countering Russian Social Media Influence, op. cit.*

plus de 150 millions de citoyens américains sur Facebook et Twitter[97]. Depuis, les plateformes américaines continuent à supprimer régulièrement des comptes contrôlés par l'IRA. Mais celle-ci cible également les réseaux sociaux russes, où elle loue l'action du Kremlin et critique ses adversaires occidentaux, en particulier l'OTAN et l'Union européenne (UE)[98]. Elle entend ainsi empêcher le rapprochement des anciennes républiques soviétiques avec l'Occident, en agissant sur les plateformes numériques russophones.

Entre 2014 et 2020, une campagne de désinformation baptisée *Secondary Infektion* s'est déroulée sur les réseaux sociaux. Les hackers à l'origine de ces manœuvres d'influence ont vraisemblablement travaillé en parallèle avec l'IRA et le GRU. La campagne, qui ciblait le plus souvent l'Ukraine, a eu recours à de faux comptes et de faux documents pour semer la zizanie entre Kiev et les pays occidentaux. Elle a produit au moins 2 500 contenus en sept langues sur plus de 300 plateformes. Si les acteurs responsables de ces opérations n'ont pas encore été identifiés, la syntaxe utilisée et le sens des messages diffusés laissent à penser qu'ils œuvraient pour les intérêts russes[99].

L'Europe et les États-Unis ne sont néanmoins pas les seuls terrains des campagnes de *trolling* russes : l'Amérique latine, le Moyen-Orient et l'Afrique sont également visés. En effet, en octobre 2019, plusieurs pages, groupes et comptes Facebook soupçonnés d'alimenter une campagne d'influence russe dans différents pays africains ont été supprimés par la plateforme[100]. En République centrafricaine, des contenus promouvant la présence russe et critiquant les actions de stabilisation française et onusienne ont été massivement diffusés sur Facebook depuis 2018[101]. Les médias russes et leurs factotums cybernétiques ont aussi joué un rôle puissant dans la campagne de dénonciation du système monétaire de la Communauté financière africaine (CFA) jouant sur les traditionnelles accusations de néo-impérialisme contre la France. Cette thématique a aussi été portée à travers le *hashtag* #boycottFrance, diffusé en République démocratique du Congo pour critiquer les contrats négociés dans le pays par le groupe Total ou encore par l'institut de formation militaire Themiis[102].

97. S. McCombie, A. J. Uhlmann et S. Morrison, « The US 2016 Presidential Election and Russia's Troll Farms », *Intelligence and National Security*, vol. 35, n° 1, octobre 2019.
98. S. Walker, « Salutin' Putin: Inside a Russian Troll House », *The Guardian*, 2 avril 2015.
99. B. Nimmo *et al.*, *Exposing Secondary Infektion: Forgeries, Interference, and Attacks on Kremlin Critics Across Six Years and 300 Sites and Platforms*, Graphika Reports, 2020.
100. « Removing More Coordinated Inauthentic Behavior from Russia », Facebook, 30 octobre 2019, disponible sur : https://about.fb.com.
101. S. Grossman, D. Bush et R. DiResta, « Evidence of Russia-Linked Influence Operations in Africa », Stanford Internet Observatory, 29 octobre 2019.
102. J.-B. Jeangène-Vilmer *et al.*, *Les manipulations de l'information*, *op. cit.*, p. 99-102.

De la même manière, le *Stanford Internet Observatory* et *Graphika* ont révélé dans un rapport de décembre 2020 que la Russie et la France se livraient une bataille d'influence sur les médias sociaux en Afrique. Dans la foulée, Facebook a annoncé avoir démantelé trois réseaux de faux comptes visant la Centrafrique, le Mali, et la Libye, dans le cadre de sa campagne de lutte contre « les comportements inappropriés et coordonnés ». Si deux de ces réseaux dépendaient de l'IRA, le dernier était vraisemblablement le fait d'individus associés aux autorités françaises, luttant contre les campagnes d'influence des trolls russes. Contrairement à ses adversaires, comme le révèle l'étude, le réseau « français » n'a pas communiqué sur la politique locale et a évité de commenter l'élection à venir. Il s'est contenté de distiller des informations sur la situation sécuritaire, en soutien aux forces armées maliennes et françaises, et en opposition aux groupes jihadistes qu'elles combattent. Cependant, comme le soulignent les experts de *Graphika* : « en créant de faux comptes et de fausses pages 'anti-fake news' pour lutter contre les trolls, les opérateurs français ont perpétué et justifié implicitement le comportement problématique qu'ils tentaient de combattre[103] ».

Chine : la propagande à la conquête du monde

Née en 1949 des fruits d'une guerre révolutionnaire, la République populaire de Chine (RPC) est sans aucun doute la grande puissance prenant le plus au sérieux les enjeux politico-militaires liés à l'influence, l'information et même la propagande puisqu'au contraire des autres cas étudiés, le terme est ouvertement revendiqué. Le Parti communiste chinois (PCC) joue un rôle fondamental dans la formulation des politiques d'influence du pays. La ligne générale est tracée lors des grands congrès quinquennaux du PCC et suivie attentivement au quotidien par le Comité permanent du Politburo qui, depuis l'installation au pouvoir de Xi Jinping, a considérablement renforcé le « travail politique », soit la propagande, l'endoctrinement idéologique et l'ingénierie du contrôle social – notamment *via* le système de crédit citoyen[104].

Les organes de la cyber-influence chinoise

L'élaboration détaillée des contenus (narratifs) revient en priorité au Groupe de pilotage de la propagande et du travail idéologique du Comité central et de son Département de la propagande qui assure un contrôle étroit des

103. « More-Troll Kombat: French and Russian Influence Operations Go Head to Head Targeting Audiences in Africa », Graphika, Stanford Internet Observatory, décembre 2020.
104. S. Arsène, « China's Social Credit System: A Chimera with Real Claws », *Asie.Visions* n° 110, Ifri, novembre 2019.

nombreux médias officiels (*Xinhua*, *China Daily*, etc.). À l'international, ces organes s'appuient ensuite sur un vaste réseau de diffuseurs et d'opérateurs sous tutelle du Bureau de l'information du ministère des Affaires étrangères et surtout du Département du travail du Front uni[105]. Placé sous l'autorité directe du Comité central, ce dernier a pris une importance considérable au cours des quinze dernières années. Il joue un rôle clé en politique intérieure en organisant la lutte contre les « cinq poisons » susceptibles selon Pékin de déstabiliser le régime et de perturber l'ordre social et politique, à la fois sur les plans national et international : la dissidence politique (libellée en Occident comme « pro-démocratie ») à Hong Kong et dans le reste du pays, la secte religieuse Falun Gong, l'indépendantisme taïwanais et les autonomismes ouïghour et tibétain[106]. Le Département du travail du Front uni travaille aussi massivement à développer l'influence chinoise à l'international. Le Front uni anime ainsi l'Association du peuple chinois pour l'amitié avec les pays étrangers et entretient des liens étroits avec les diasporas chinoises d'outre-mer. Il contribue aussi à la gouvernance des médias après avoir pris le contrôle en 2018 du deuxième groupe de presse du pays, le *China News Service*[107].

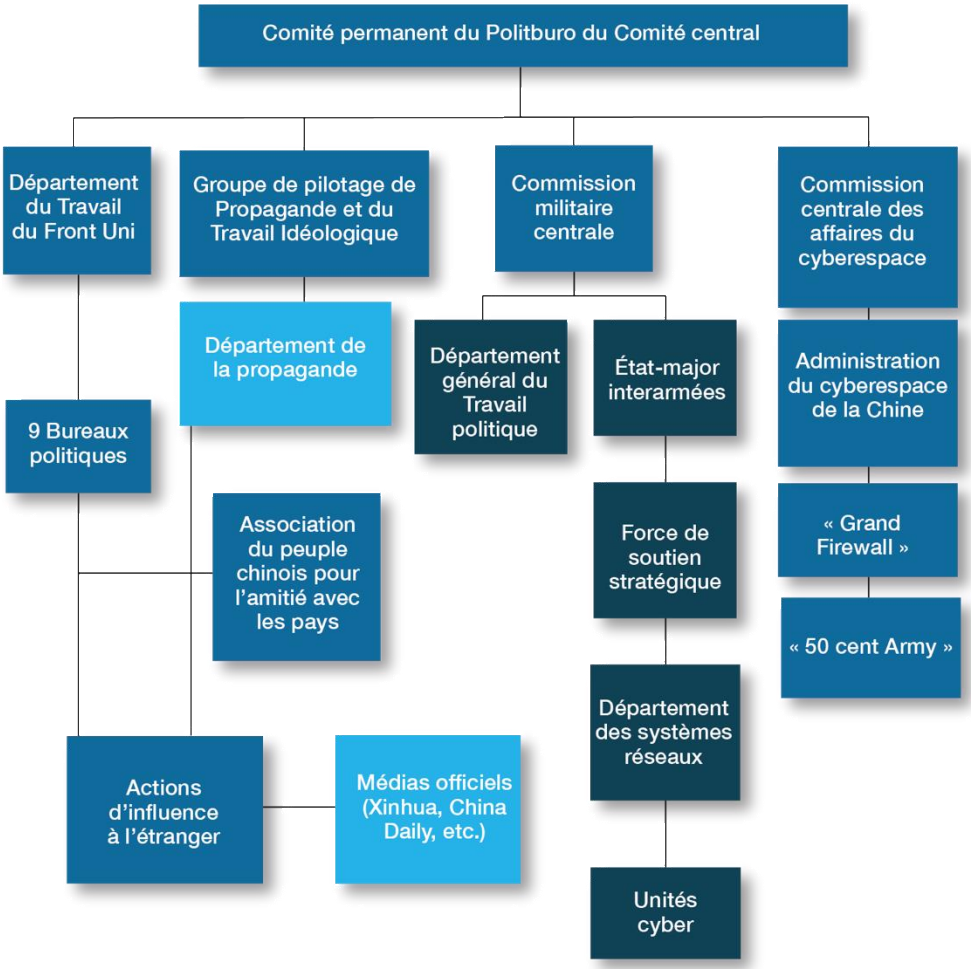
Tout comme la Russie, la Chine se considère comme la victime de campagnes systématiques de cyber-influence venues du monde occidental, se cachant derrière la façade d'ONG militant pour les droits de l'homme et de médias critiques du régime. Afin de se prémunir contre cette menace, le pays s'est doté de protections techniques et juridiques pour assurer le filtrage de l'information accessible depuis son réseau Internet. Surnommé le « *Grand Firewall* », ce projet de surveillance et de censure, initié dès 1998, exerce un contrôle sur les couches basses du cyberespace (blocage d'adresses IP, filtrage des DNS, des URL et des paquets TCP[108]). Ce dispositif de censure sans équivalent dans le monde est piloté, depuis 2018, par la Commission centrale des affaires du Cyberespace, présidée par Xi Jinping en personne.

Bien qu'elle ne soit pas autorisée à prendre l'initiative des campagnes d'influence, l'Armée populaire de libération (APL) sert de bras armé au pouvoir, en diffusant massivement ses narratifs sur des canaux d'information intérieurs et extérieurs. Placé sous l'autorité de la Commission militaire centrale à rang égal de l'état-major interarmées, le Département du Travail

105. M. Stokes et R. Hsiao, « The People's Liberation Army General Political Department: Political Warfare with Chinese Characteristics », Arlington, VA, Project 2049 Institute, 14 octobre 2013.
106. K. Gordon, « China's Fifth Poison », *Issues Brief*, Canberra, Australian Institute of International Affairs, 2 mai 2014.
107. S. Hoffman et P. Mattis, « Managing the Power Within: China's State Security Commission », *War on the Rocks*, 18 juin 2016, disponible sur : https://warontherocks.com.
108. J. Costello, « Chinese Views on the Information 'Center of Gravity': Space, Cyber, and Electronic Warfare », *China Brief Volume*, vol. 15, n° 8, Washington, DC, Jamestown Foundation, avril 2015.

politique de l'armée joue un rôle clé dans la formulation des missions de l'APL dans l'environnement informationnel intérieur. C'est cette structure qui a formalisé le principe des « trois guerres » : la guerre de l'opinion publique visant les audiences nationales et internationales à travers les relais médiatiques ; la guerre psychologique, directement conduite contre les forces adverses ; et enfin la guerre juridique (*lawfare*), destinée à délégitimer l'ennemi sur le plan du droit international[109]. Dans cette perspective, l'information est pleinement intégrée aux attributs de la puissance militaire chinoise, et la numérisation transforme sa manière de faire la guerre[110].

Schéma n° 5 : Architecture simplifiée de la cyber-influence en Chine



En ce qui concerne les capacités d'action militaire dans le cyberespace, longtemps dispersées au sein de l'APL, ces dernières sont aujourd'hui

109. *La Défense nationale de la Chine à l'ère nouvelle*, Bureau d'information du Conseil d'État, République populaire de Chine, juillet 2019.
110. A. Crowther, B. Fonseca, K. Green, R. Morgus, « Are China and Russia on the Cyber Offensive in Latin America and the Carribean? », *Florida International University*, 26 juillet 2019.

rassemblées après la création en décembre 2015 de la Force de soutien stratégique (FSS). Avec un effectif de plus 175 000 hommes, ce fer de lance des capacités technologiques intègre sous un seul commandement les capacités spatiales et cyber. C'est le Département des Systèmes et Réseaux qui concentre les activités dans le cyberespace avec les 3e et 4e départements du renseignement de l'APL, et qui conduit les opérations de cyber-espionnage et d'attaques techniques ou informationnelles[111].

Enfin le pouvoir chinois, dont le développement capacitaire est fortement marqué par le dualisme civilo-militaire, travaille en étroite collaboration avec des acteurs privés. Il s'appuie en particulier sur la *China Electronics Technology Corporation* (CETC) et des instituts de recherche tels que l'Université des sciences et technologies de Pékin, afin de se doter des dernières innovations dans le domaine de la cyber influence. En 2018, l'APL a ainsi annoncé travailler à la densification des capacités opérationnelles dans la dimension cognitive de l'environnement informationnel, en particulier en ce qui concerne les réseaux sociaux, le *big data,* l'apprentissage profond, l'analyse comportementale et le traitement automatique du langage naturel. À terme, ces recherches doivent permettre à la Chine de recourir en ligne aux messages subliminaux et à la synthèse vocale, à des fins de propagande[112].

Diplomatie publique et « nation branding »

L'influence chinoise dans le cyberespace vise d'abord à promouvoir l'image de la Chine dans le monde. À cet égard, les médias sociaux tels que Weibo et WeChat sont très largement utilisés pour diffuser les narratifs du pouvoir auprès du public chinois, mais aussi vers la diaspora sinophone à l'étranger. Les autorités chinoises ont également recours à des plateformes américaines comme Facebook et Twitter pour atteindre des audiences internationales. En août 2019, Twitter a révélé avoir supprimé pour la première fois 936 comptes de *bots* ou de *trolls* chinois. Puis en juin 2020, 173 550 autres comptes ont été effacés lors d'une opération « coup de poing ». Un dixième de ces comptes était utilisé pour élaborer des contenus en faveur de Pékin, et les 90 % restants servaient à les amplifier. Il apparaît que ces comptes, qui publiaient en chinois, ciblaient la diaspora sinophone dans le monde[113].

111. E. Kania, « The Role of PLA Base 311 in Political Warfare Against Taiwan (Part 3) », *Global Taiwan Brief*, vol. 2, n° 7, Washington, DC, Global Taiwan Institute, 15 février 2017.
112. L. Xiong *et al.*, « Several thoughts on Promoting the Construction of Cognitive Domain Operations in the Whole Environment », *Defense Technology Review*, octobre 2018.
113. Twitter Safety, « Disclosing Networks of State-linked Information Operations We've Removed », *Blog Twitter*, 12 juin 2020, disponible sur : https://blog.twitter.com.

Pour appuyer ses opérations d'influence, le PCC s'appuie en outre sur un très grand nombre de commentateurs en ligne. Ces derniers ont pu être qualifiés « d'armée des 50 centimes » parce qu'ils seraient rémunérés cinquante centimes de yuan pour chaque publication. Ils produisent et diffusent en ligne des contenus favorables aux autorités chinoises, et répondent à ceux qui critiquent le gouvernement sur les réseaux sociaux, tant chinois qu'internationaux[114].

Discréditer ses adversaires

Parallèlement aux actions de défense informationnelle de la position chinoise, Pékin pratique aussi l'attaque, notamment en vue de discréditer ses adversaires. À l'automne 2019, une campagne d'influence a ainsi été conduite pour dénigrer les revendications des manifestants à Hong Kong et légitimer la mobilisation de l'APL et des forces paramilitaires. À cette fin, des comptes institutionnels chinois ont diffusé sur les réseaux sociaux de fausses informations sur le saccage des rues par les manifestants, et leur nettoyage par l'APL. Ces fausses informations ont été relayées sur Weibo, puis reprises par les médias officiels nationaux et internationaux[115].

La lutte contre la pandémie de COVID-19 a également été l'occasion d'une campagne d'influence massive visant à façonner un narratif global favorable à la Chine quant à l'origine du virus, et à inspirer la méfiance vis-à-vis des États-Unis. Ainsi, le 13 mars 2020, Zhao Lijian, vice-directeur du Bureau de l'information du Ministère des Affaires étrangères a partagé sur Twitter un article conspirationniste laissant entendre que le coronavirus avait été créé dans un laboratoire de l'armée américaine et importé en Chine en novembre 2019, lors des Jeux olympiques militaires. Dans les jours qui ont suivi, le compte Twitter de Zhao Lijian, sur lequel il a déjà répandu maintes fois ce genre de fausses informations, a vu son nombre de nouveaux *followers* par jour multiplié par vingt. Or, près de la moitié des nouveaux comptes étaient des *bots* ou des *trolls* conçus spécialement pour propager et amplifier ce contenu dans les pays occidentaux[116]. Le but de ces activités de désinformation est de créer de la confusion dans le camp adverse pour influencer ses perceptions, afin que soient prises des décisions favorables à la Chine.

114. G. King, J. Pan et M. E. Roberts, « How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument », *American Political Science Review*, vol. 3, n° 111, 2017.
115. S. Lagarde, « Hong Kong : l'armée intervient pour nettoyer les rues, une présence symbolique », *RFI*, 16 novembre 2019, disponible sur : www.rfi.fr.
116. J. Hansler, « Twitter Disputes State Department Claims China Coordinated Coronavirus Disinformation Accounts », *CNN*, 8 mai 2020, disponible sur : https://edition.cnn.com.

Appuyer des revendications territoriales

Les opérations d'influence de la Chine dans le cyberespace servent aussi à appuyer ses revendications territoriales, notamment par la diffusion de fausses informations (sur Hong Kong et Taïwan en particulier). Ainsi, à l'été 2016, après que la Cour permanente d'arbitrage du Tribunal de La Haye a tranché en défaveur de Pékin quant à la souveraineté sur le récif de Scarborough, en mer de Chine méridionale, des dizaines de sites gouvernementaux philippins, dont celui du ministère de la Défense, ont subi des attaques DDoS, puis ont été défacés. Trois jours plus tard, un bombardier H-6K a survolé le récif, et l'armée de l'Air chinoise (PLAAF) a publié une photographie du vol sur son compte Weibo. Les médias anglophones chinois ont ensuite largement partagé cette photographie, notamment sur Twitter. Cette opération a permis de contester sur le plan informationnel la décision juridique de la CPA – soulignant ainsi l'interdépendance des « trois guerres[117] ».

Le même type de manœuvre d'intimidation a été exercé à l'encontre de Taïwan en décembre 2017, lorsque la PLAAF a publié sur son compte Weibo la photographie du survol d'une île, que les internautes étaient invités à identifier. En reconnaissant une île administrée par Taïwan, les internautes ont amplifié la publication, qui a en outre bénéficié d'une large couverture médiatique nationale. Ce type d'opérations d'influence dans le cyberespace permet en outre de mettre en avant la modernité et la puissance de l'APL.

117. C. Cimpanu, « Philippines Government Website Hit by Massive DDoS Attacks, China Suspected », *Softpedia News*, 18 juillet 2016, disponible sur : https://news.softpedia.com ; China State Council Information Office, « Some Photos Brought By PLA Air Force: Bomber H-6K Fly over Huangyan Island », *Twitter*, 15 juillet 2016, disponible sur : https://twitter.com.

Le bel avenir de la guerre de l'information

Les capacités déterminantes demain

L'environnement technologique du cyberespace évolue à un rythme effréné, porté par la croissance continue de l'économie numérique et la plasticité des langages et des plateformes d'action. De ce fait, l'irruption de nouveaux acteurs et de nouvelles pratiques devrait rester la règle dans un contexte où le coût d'entrée tout comme les risques demeurent relativement réduits alors que les possibilités de gains sont très élevées. Les actions d'influence sont l'exemple même de cette stratégie indirecte qui continuera selon toute vraisemblance à prévaloir dans les conditions actuelles des rapports de force internationaux. Même dans la perspective d'un conflit ouvert, limité mais de « haute intensité[118] » capacitaire, le volet informationnel permettra de plus en plus de contraindre les options d'un adversaire pour faire émerger un rapport de force plus favorable, ou d'asseoir sa supériorité sans même agir sur le terrain militaire.

L'intelligence artificielle

L'intelligence artificielle (IA), qui désigne l'ensemble des techniques mises en œuvre afin de permettre aux machines de simuler l'intelligence, est probablement le domaine technologique qui suscite le plus d'attente pour les décennies à venir. Le domaine de l'influence militaire n'échappe pas à la règle : les possibilités offertes par l'IA sont nombreuses, en ce qu'elle permet de simuler des réponses « intelligentes » à la réception et au traitement de l'information. En cherchant à copier et à reproduire de façon de plus en plus fine – en intégrant de plus en plus de données – un comportement humain apparemment authentique, les algorithmes intelligents contribueront à automatiser de nouvelles tâches et à améliorer les outils de cyber-influence déjà opérationnels. Par exemple, grâce aux avancées du *machine learning*,

118. M. Pesqueur et É. Tenenbaum, « Les défis de la 'haute intensité' : enjeu stratégique ou capacitaire ? », *Cahier de la RDN - La vision stratégique de l'Armée de Terre*, 2020, p. 11-17.

les *bots* pourront mieux maîtriser la langue et la culture de leur audience cible, ce qui les rendra plus crédibles, et donc moins détectables[119].

En outre, dans des domaines tels que la reconnaissance de la parole ou de motifs, le choix stratégique, la perception visuelle et la traduction, l'IA devrait faire figure de véritable *game changer* dans les années à venir. D'après les estimations, les développements futurs de l'IA incluent le traitement simultané d'une masse de plus en plus complexe d'informations, ainsi la reconnaissance de plus en plus fine des images et des sons grâce au *deep learning* et aux réseaux de neurones. Cela ouvre des possibilités dans le domaine de la perception auditive et du *natural language processing* (traitement automatique du langage). Dans cette perspective, l'IA pourra être utilisée pour interagir avec une audience cible de manière indétectable, grâce aux progrès des agents conversationnels (*chatbots*), et créer des polémiques ou envenimer des débats sur les plateformes numériques afin d'exacerber les fractures sociales, ou discréditer une force par exemple[120]. Ces agents conversationnels seront aussi utiles pour la collecte de renseignements sur les réseaux. De la même manière que des membres du Hamas piégeaient des soldats israéliens sur des applications de rencontre (*cf. supra*), des *chatbots* aux avatars attrayants pourraient engager massivement des militaires sur les réseaux, afin de recueillir des informations contextuelles ou sur leur état moral. Dans la logique du *cyborg*, ces logiciels automatisés pourraient préparer le terrain et présélectionner les cibles pour un traitement humain plus personnalisé.

Inversement, l'IA devrait aussi fournir des instruments de plus en plus performants pour détecter les tentatives d'intrusion, de manipulation de l'information ou les comportements adverses visant à provoquer des effets non désirés dans le cyberespace. La prise de décision algorithmique permettra par ailleurs de faire des prévisions et des estimations des campagnes d'influence adverses, afin d'anticiper les menaces. Les grandes plateformes du web utilisent d'ores et déjà des outils automatisés pour participer à la régulation des activités de leurs utilisateurs et même à anticiper en amont les thématiques susceptibles de s'imposer dans les jours et semaines à venir – une fonctionnalité également en plein essor chez les communicants spécialistes de la veille réputationnelle[121]. Dès lors, les armées et les services spécialisés pourraient détecter dès les premiers signaux faibles le déclenchement d'une campagne de désinformation, visant une opération ou un déploiement à l'étranger, et ainsi préparer une

119. J. Marceau, « Intelligence artificielle : le numérique ne doit pas devenir 'l'objet de tous les doutes' », *Le Monde*, 29 février 2020.
120. M. J. Mazars *et al.*, *The Emerging Risk of Virtual Societal War*, Santa Monica, CA, RAND Corporation, 2019.
121. M. Cherki, « Des chercheurs prédisent les tendances à venir sur Twitter », *Le Figaro*, 7 novembre 2012.

campagne de contre-influence, par exemple en noyant les contenus hostiles dans une masse d'autres messages sur le même thème. Lors du récent conflit dans le Haut-Karabakh, au cours duquel l'Azerbaïdjan a vraisemblablement eu recours à des méthodes d'*astroturfing* sur Twitter pour faire croire qu'elle bénéficiait de davantage de soutiens organiques qu'elle n'en avait vraiment[122], l'Arménie aurait pu mener une contre-campagne grâce à ces outils, en détournant et noyant les *hashtags* #StopArmenianAgression, #StopArmenianOccupation, #KarabakhIsAzerbaijan et #ireli2020 avec des contenus absurdes pour qu'ils ne deviennent pas des tendances sur le réseau social.

Cette instrumentalisation massive du cyberespace ne manquera pas de susciter l'inquiétude des défenseurs de la liberté d'expression et de la neutralité du Net. Il n'en demeure pas moins qu'il s'agit d'une évolution probable du cyberespace, au vu des investissements massifs décrits ici par des acteurs étatiques décidés à ne pas laisser s'imposer la spontanéité des utilisateurs. Ainsi l'Internet qui était jusqu'à présent marqué par les interactions « d'humain à humain » par l'intermédiaire de machines, sera de plus en plus marqué par l'interaction d'« humain à machine » et même de « machine à machine », les programmes défensifs s'interposant à chaque fois qu'un programme offensif cherche à intervenir et à l'inverse, les programmes offensifs s'ajustant pour ne plus être détectés par les programmes défensifs.

L'hyperpersonnalisation

Si la personnalisation des opérations d'information a toujours été l'un des leviers de l'influence, la transformation numérique a permis de la combiner avec un effet de masse tout à fait inédit, comme en attestent tous les jours les procédés de marketing ciblés à partir des données personnelles hébergées et commercialisées par les grandes plateformes du web social. Les scandales à répétition causés par l'utilisation de ces données à des fins de « marketing politique » (c'est-à-dire de propagande) par la firme Cambridge Analytica ont démontré la puissance de cette personnalisation pour affecter les perceptions et *in fine* les comportements sur des enjeux plus larges que de simples produits de consommation.

Des cas encore rares attestent de l'exploitation de cette logique dans le cadre de conflits armés, comme cela a pu déjà être le cas en Ukraine par exemple. Les techniques de personnalisation des messages, souvent sur les plateformes numériques et les messageries instantanées, permettent déjà de cibler toujours plus efficacement les individus. Demain, le développement

122. Z. Kharazian, « Patriotic Astroturfing in the Azerbaijan-Armenia Twitter War », Washington, DC, Atlantic Council's Digital Forensic Research Lab, 1er octobre 2020.

de technologies telles que le *neurohacking*, la reconnaissance faciale et la reconnaissance émotionnelle favoriseront une indentification extrêmement fine des individus ciblés, et une adaptation à leurs réactions[123]. En effet, en examinant la réaction d'un public à une campagne, ces outils permettent de saisir très finement l'impact visuel, émotionnel, rationnel, et intellectuel d'un message sur une audience spécifique. De plus, en analysant les raisons pour lesquelles un individu s'approprie un message plutôt qu'un autre, ils renseignent sur la manière dont les campagnes d'influence dans le cyberespace peuvent accroître leur attractivité et retenir l'attention d'une audience qui leur échappe.

Des technologies comme l'analyse du regard (*eye tracking*), utilisée initialement pour renforcer la vigilance au volant, permettent aussi d'entrer dans l'intimité des utilisateurs, et de les saisir au moment où ils sont le plus concentrés, et adapter les narratifs qui leur sont présentés pour maintenir leur attention. Les techniques d'optimisation de la captation de l'attention *via* l'exploitation des neurosciences (activation du circuit de la récompense), déjà employées massivement pour la diffusion de jeux vidéo et de publicités digitales, pourraient également servir à renforcer l'emprise d'une manœuvre donnée sur sa cible. Grâce à l'exploitation de données personnelles enfin, les cibles – militaires, décideurs, etc. – pourraient être visées par des opérations d'influence « sur-mesure », au moment où ils sont les plus vulnérables émotionnellement, à partir de références qui les touchent particulièrement, afin d'infléchir leurs opinions ou de prédisposer leurs actions. Il serait alors possible d'intoxiquer les membres d'une unité, en les incitant à dévoiler leur position, capituler ou déserter.

L'hyperpersonnalisation de la stratégie d'influence sera encore renforcée par le développement de l'Internet des objets (IoT) qui facilite le travail préparatoire d'analyse de l'audience cible (collecte du renseignement). Ainsi, l'identification des *patterns* pourra s'étendre à de nouveaux domaines grâce aux progrès en domotique. D'après les estimations de la RAND Corporation, il y aura d'ici 2030 plus de 1 000 milliards de capteurs connectés à l'IoT, ce qui représentera plus de la moitié du trafic Internet depuis et vers des logements[124]. Dans les régimes autoritaires, ces développements pourraient même faire de l'IoT un outil de surveillance des opinions subversives, pour assurer la « solidité des arrières ». À terme, on peut craindre l'avènement d'un « système de surveillance ambiant », qui permettrait par exemple de repérer les moments de disponibilité d'une audience cible à partir de ses habitudes, ou d'enregistrer des conversations privées grâce aux assistants virtuels (tels

123. *Ibid.*
124. *Ibid.*

que Google Home ou Alexa d'Amazon) pour ensuite les diffuser sur le web. La méthode du *hack and leak* prendrait alors une nouvelle dimension.

La modification de contenus

Les techniques de modification des contenus ne cessent de s'améliorer. Ainsi Adobe, Lyrebird ou VivoText proposent d'ores et déjà des solutions pour faire prononcer un discours par une voix virtuelle. Demain, les logiciels d'édition photo, audio et vidéo, permettront de faire dire ce que l'on veut à qui l'on veut, de manière de plus en plus difficilement détectable. La technologie du *deepfake* consiste ainsi à retoucher numériquement des fichiers vidéo à partir d'algorithmes intelligents nourris de données suffisamment fines pour renforcer la crédibilité du montage. Pour faire face à ces défis, la Defense Advanced Research Projects Agency (DARPA) a d'ailleurs apporté des fonds au *Media Forensics Project*, qui vise à développer une technologie capable de repérer automatiquement ces trucages. Mais les contenus audios ou vidéos pourraient aussi être seulement en partie falsifiés, ce qui rendrait les tentatives d'influence plus discrètes et subtiles, et donc plus dangereuses. Des dizaines de variantes d'un contenu officiel pourraient alors être diffusées et amplifiées, afin de diluer le discours authentique[125]. À cet égard, les technologies de réalité virtuelle et de réalité augmentée offrent de nombreuses possibilités.

Entre 2015 et 2016, l'escroquerie dite du « Faux Le Drian », avait mis en scène de faux appels du ministre de la Défense, dans le but d'extorquer des fonds à des personnalités, des ambassadeurs et des hommes d'affaires[126]. En leur faisant croire que le ministre avait besoin de cet argent pour payer la rançon d'otages français aux mains de djihadistes, les malfaiteurs étaient parvenus à extorquer plus de 80 millions d'euros. À l'époque, les escrocs avaient fabriqué un masque de Jean-Yves Le Drian en silicone pour duper leurs cibles sur Skype[127]. Mais incessamment, les techniques de *deepfake* pourraient permettre d'initier des attaques semblables, de manière encore plus crédible. Or, on imagine sans peine les conséquences dramatiques que pourrait avoir la vidéo d'un chef d'état-major prêchant un discours de haine, ou de soldats perpétrant des exactions sur des populations civiles au cours d'une opération extérieure. Bien sûr, de telles opérations pourraient avoir des conséquences très néfastes sur le rapport des armées avec les populations (dans le cas d'une vidéo montrant des exactions supposément conduites par une armée partenaire dans un pays hôte par exemple), ou

125. J.-B. Jeangène-Vilmer *et al.*, *Les manipulations de l'information*, *op. cit.*
126. S. Piel, « Masque de ministre, fausse boîte mail, prétendue rançon…l'arnaque au faux Le Drian devant la justice », *Le Monde*, 4 février 2020.
127. *Ibid.*

encore sur le moral des troupes (avec des sons ou des vidéos montrant l'absence de soutien à leur action de la part des décideurs politiques ou militaires).

De surcroît, même si l'origine frauduleuse de ces contenus était prouvée, leur impact n'en demeurerait pas moins immense. En effet, la particularité des fausses informations est de survivre à leur démenti ou à la démonstration de manipulations[128]. Certains voient même dans les efforts de *fact checking* des preuves de complots. De plus, les *fake news* tendent à être davantage partagées que les informations réelles, ce qui explique leur très forte viralité et donc leur utilité en termes de stratégie d'influence[129]. Dans cette perspective, l'offensive informationnelle aurait l'avantage sur la défensive, dans la mesure où la vérification des faits prend du temps et se diffuse avec une efficacité moindre. Au contraire, les initiatives permettant d'identifier en amont les messages manipulés sont susceptibles de rétablir l'équilibre en faveur de la défensive. Les implications de ces caractéristiques en termes d'équilibre offensif/défensif ne sauraient alors être négligées. En outre, elles permettent en partie d'expliquer l'affaiblissement de la portée des argumentaires et la défiance envers les faits communiqués par les institutions, mais aussi la montée continue des thèses « alternatives » et du conspirationnisme – autant de variables sur lesquelles s'appuient les acteurs de la lutte informationnelle cyber pour exacerber la réceptivité des audiences cibles.

La blockchain*, un outil de lutte contre la manipulation ?*

Les technologies émergentes, si elles sont porteuses de risques et de menaces, pourraient aussi être en mesure d'aider les armées à lutter contre les manœuvres d'influence dans le cyberespace. À ce titre, l'utilisation de la technologie dite de la chaîne de blocs (*blockchain*), qui permet d'améliorer la traçabilité de l'information, gagnerait à être explorée.

En effet, la *blockchain* est une technologie de stockage et de transmission d'informations. Elle est transparente, sécurisée par cryptographie, et fonctionne sans organe central de contrôle[130]. Par extension, elle renvoie à une base de données contenant l'historique de tous les échanges survenus entre ses utilisateurs, et ce depuis sa création. Cette base est sécurisée, et partagée par tous les utilisateurs sans

128. H. Allcott et M. Gentzkow, « Social Media and Fake News in the 2016 Elections », *Journal of Economic Perspectives*, vol. 31, n° 2, Printemps 2017.
129. C. Silverman, « This Analysis Shows how Fake Election News Stories Outperformed Real News on Facebook », *BuzzFeed News*, 16 novembre 2016, disponible sur : www.buzzfeednews.com.
130. « Blockchains: The Great Chain of Being Sure about Things », *The Economist*, 31 octobre 2015.

intermédiaire, ce qui garantit à chacun la validité de la chaîne. Si elle est publique, une *blockchain* s'apparente alors à un immense livre comptable public, anonyme et infalsifiable. Dans cette perspective, la technologie de la *blockchain*, parce qu'elle est décentralisée, sécurisée et transparente, pourrait prétendre à des applications bien plus larges que le seul domaine monétaire[131]. Bien qu'elle soit extrêmement consommatrice de ressources au regard de la volumétrie de transaction, elle pourrait émerger comme un moyen de suivre la temporalité, les méthodes et les acteurs de communication, et donc de se prémunir de manœuvres de cyber-influence adverse.

Les enjeux pour la France : un nécessaire *aggiornamento* stratégique

Du fait de son statut de puissance d'influence mondiale, de son siège permanent au Conseil de sécurité de l'Organisation des Nations unies, et de son poids au sein de l'OTAN et de l'UE, la France est aujourd'hui une cible privilégiée de campagnes continues d'influence, de lutte informationnelle et de déstabilisation menées depuis le cyberespace. La prise de conscience s'est amorcée, et le rapport sur les *Manipulations de l'information* co-publié à l'été 2018 par l'Institut de recherche stratégique de l'École militaire (IRSEM) et le Centre d'analyse, de prévision et de stratégie (CAPS) s'en est fait l'écho, dressant un constat alarmiste de l'ampleur des défis en la matière et soumettant cinquante recommandations concrètes pour les services de l'État, en vue de préparer la France à une menace qui n'a pu qu'être confirmée depuis lors.

Il serait faux de dire que les cris d'alerte n'ont pas été suivis d'effets. Le vote en novembre 2018 d'une loi contre la manipulation de l'information a doté les pouvoirs publics des moyens juridiques de poursuivre la diffusion massive ou automatisée d'informations manifestement fausses dans le but de troubler la paix publique ou la sincérité d'un scrutin. Le Secrétariat général à la Défense et à la Sécurité nationale (SGDSN) a pour sa part produit la même année une *Revue stratégique de cyberdéfense*, tandis que le ministère des Armées a publié en 2019 une nouvelle doctrine de cyberdéfense, déclinée en une « Politique ministérielle de lutte informatique défensive » et des « éléments publics de doctrine militaire de lutte informatique offensive ». Enfin sur le plan des capacités, la loi de Programmation militaire (LPM) 2019-2025 a érigé en priorité le développement de moyens supplémentaires dans le domaine de « la cyberdéfense et de l'action numérique » avec la création de 1 500 postes supplémentaires dans ces secteurs. En octobre 2020,

131. A. Reverchon, « Blockchain : sécurité des données pour les uns, indépendance pour les autres », *Le Monde*, 25 septembre 2019.

Marlène Schiappa a en outre présenté une nouvelle proposition pour endiguer les discours djihadistes sur les plateformes numériques. Elle a en effet annoncé la création d'une unité de contre-discours républicain sur les réseaux sociaux, sous l'autorité du Comité interministériel de prévention de la délinquance et de la radicalisation (CIPDR), dirigé par le préfet Christian Gravel[132].

Si le défi de développer un outil technique performant sur les plans défensif et offensif, à la hauteur des ambitions françaises en matière de lutte informatique, semble en passe d'être relevé, force est de constater que l'organisation de la lutte informationnelle dans le cyberespace (LIC) en France semble aujourd'hui en décalage avec les moyens mis en œuvre par les grands acteurs du domaine tels que ceux évoqués dans cette étude. Nous proposons ici de présenter quelques recommandations dans le champ de la doctrine, de l'organisation, des ressources et de l'équipement applicable aux armées. La problématique de la cyber-influence étant par éminence transverse et interarmées, il paraît illusoire de proposer des recommandations propres à chaque armée. Il est dans l'intérêt de toutes les armées de s'impliquer davantage dans ce domaine de lutte.

Faire émerger une chaîne de communication stratégique intégrée

Contrairement à ce que préconisait le rapport CAPS-IRSEM il y a deux ans, aucune structure dédiée permanente n'a été créée pour prendre en compte ces questions, et la notion de « communication stratégique » prônée à l'OTAN n'a toujours pas d'équivalent à l'échelon interministériel en France. Il existe plusieurs instances abordant ces questions au travers d'un portefeuille plus large. Ainsi, au sein du ministère de l'Europe et des Affaires étrangères, l'Ambassadeur pour le numérique œuvre à la lutte contre les fausses informations et la radicalisation en ligne. Il n'existe toutefois pas d'instance en charge de la diplomatie publique ni d'équivalent du *Global Engagement Center* américain. De même, le Service d'information du gouvernement, placé sous l'autorité du Premier ministre, a joué un rôle important en organisant la campagne de prévention de la radicalisation #StopJihadisme mais semble avoir perdu en importance au cours des dernières années. Aucune de ces structures n'a cependant de mandat explicite sur la question, ni de moyens spécifiques à y consacrer. Il en va de même du SGDSN qui a pu récemment mettre en place un groupe de travail sur la lutte contre la cyber-influence mais qui n'a pas de capacité de décision propre.

132. M. Delahousse et M. Thierry, « Marlène Schiappa annonce la création 'd'une unité de contre-discours républicain sur les réseaux sociaux' », *L'Obs*, 23 octobre 2020.

Les armées doivent donc mettre en œuvre la stratégie militaire d'influence sans directive ni coordination systématique avec les autres organes gouvernementaux. La communication institutionnelle et la communication opérationnelle relèvent respectivement de la Direction de la communication de la Défense et de l'état-major des armées. Ces dernières n'entretiennent pas de lien direct avec la stratégie militaire d'influence qui est formulée par le bureau « influence militaire » (J-IM) du Centre de planification et de conduite des opérations (CPCO). Cette cellule, qui sert de conseiller influence militaire du CEMA, contribue aussi depuis Paris aux processus de « ciblage large spectre » (J-CLS) qui implique également la DRM et le Centre national de ciblage. Le JIM repose sur le bras armé que constitue le Centre interarmées des actions sur l'environnement (CIAE). Basé au Quartier général-Frère à Lyon, le CIAE dépend organiquement du commandement renseignement de l'armée de Terre, assure une formation continue des armées aux opérations d'information et fournit au CPCO les ressources nécessaires aux déploiements opérationnels.

Cette approche traditionnelle orientée vers la projection sur un théâtre d'opérations est aujourd'hui partiellement remise en cause par la montée en puissance parallèle de la lutte informationnelle cyber – notamment à l'occasion des moyens supplémentaires dégagés par la LPM 2019-2025 – conduite directement depuis le territoire national. Cette dernière est pilotée, aux côtés des unités de lutte informatique offensive et défensive, par le Commandement de la Cyberdéfense (COMCYBER), placé directement sous l'autorité du sous-chef opérations de l'EMA. Le COMCYBER dispose d'une capacité opérationnelle d'une centaine d'opérateurs évoluant dans la sphère cognitive du cyberespace. Ces derniers assurent des fonctions de veille, d'analyse et d'action sur ce segment.

Ce dispositif permet aujourd'hui une veille des actions d'influence « d'intérêt militaire » concernant les armées françaises, des planifications de CLS en anticipation visant, difficilement compte tenu de l'hétérogénéité des logiques, à intégrer l'influence avec les effets et les actions cinétiques et cyber plus disruptives, ainsi qu'à appuyer les forces en opération sur des besoins précis et ciblés. Il est toutefois important de prendre en compte que l'horizon opérationnel de ces deux dernières décennies a été essentiellement dominé par les opérations de lutte contre le terrorisme. Si les groupes djihadistes ont démontré un activisme particulièrement virulent dans le cyberespace, leurs moyens ne peuvent en aucune façon être comparés à ceux mis en œuvre par des acteurs étatiques tels que la Chine, la Russie voire l'Iran. Les limites du dimensionnement français actuel en termes de lutte informationnelle cyber ont même été ressenties à la suite des tensions militaires avec la Turquie à l'été et l'automne 2020.

La spécificité de la cyber-influence dans ce nouveau cadre de la compétition stratégique entre puissances est de se dérouler en dehors du cadre du droit des conflits armés, plaçant donc l'architecture militaire française à l'écart de la plupart des actions possibles. Cette problématique de la « zone grise » renvoie de façon impérieuse au manque de coordination – et même de hiérarchie – interministérielle, laissant aujourd'hui l'outil militaire dépourvu de directive stratégique. Il est donc urgent de créer la « structure dédiée » déjà recommandée dans le rapport CAPS-IRSEM de 2018. Cette dernière pourrait se placer dans le cadre d'une revalorisation du rôle du Service d'information du gouvernement (SIG) avec des attributions interministérielles. Un élargissement des compétences de l'Agence nationale de sécurité des systèmes d'information (ANSSI) pour inclure la lutte contre la manipulation de l'information pourrait aussi être envisagé. Enfin une réforme du SGDSN, potentiellement rapproché du Coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT) sous une houlette présidentielle, pourrait conduire à l'émergence d'une nouvelle instance capable de conduire l'action de l'État dans les nouvelles « zones grises » de la conflictualité contemporaine.

Revaloriser la place de l'influence dans les armées

Même si dans les faits le parcours de certains officiers français est marqué par la problématique de l'influence militaire et des opérations d'information, il n'existe pas à ce jour de filière ou de spécialisation – à l'instar de l'artillerie ou de la sous-marinade, ou des opérations spéciales – qui puisse assurer une reconnaissance et une mémoire institutionnelle pérenne des compétences associées. Les officiers rencontrés et responsables de cette fonction jugent toutefois qu'il est bénéfique que cette dernière ne devienne pas un « métier » au sein des armées, afin de faciliter son appropriation par l'ensemble des forces impliquées dans les opérations.

Force est pourtant de constater que la fonction influence militaire souffre en France aujourd'hui d'une certaine marginalité bureaucratique. Tandis qu'au sein de l'armée britannique une brigade entière – la 77e « Chindits » – est en charge des opérations d'information, elle-même au sein d'une 6e Division entièrement orientée vers les champs immatériels (guerre électronique, partenariat militaire opérationnel), les plus hauts responsables français, organiques et opérationnels, dans le domaine n'occupent que le grade de colonel (qu'il s'agisse du J-IM ou du ComCIAE). Certains observateurs avisés estiment que cette place s'est encore réduite au cours des dernières années. Ainsi alors qu'en 2010 la *task force* « La Fayette » en Afghanistan comptait 24 personnels dédiés aux seules opérations

psychologiques, la force *Barkhane* en 2020 ne compterait plus que 10 militaires dédiés à cette fonction.

La raison de ce sous-développement tient à plusieurs facteurs : la sensibilité politique dont cette fonction fait l'objet est tant le produit de l'histoire française, et notamment de la mémoire douloureuse des 5e Bureaux durant la guerre d'Algérie, que d'un découplage fort entre les décideurs politiques et diplomatiques d'une part et les acteurs militaires d'autre part qui conçoivent leur métier comme celui de « techniciens de la violence ». Les évolutions de la conflictualité doivent cependant amener les armées à revisiter ces postulats et cet héritage pour réinvestir ce champ – et ce dans un périmètre qui devra avoir été redéfini par des arbitrages interministériels encore dans les limbes (*cf. supra*).

En attendant cette revalorisation nécessaire, des évolutions plus pragmatiques peuvent être envisagées sur le plan de l'intégration à la chaîne de conduite et de planification opérationnelle. C'est tout particulièrement le cas du lien avec l'appui renseignement. Il apparaît que la ligne « influence » est insuffisamment prise en compte dans le schéma d'orientation renseignement d'intérêt militaire – souvent considéré comme trop focalisé sur l'appui aux effets cinétiques – alors même qu'une opération d'information ne peut être montée sans un travail préparatoire d'analyse de l'audience cible (et donc de renseignement). En l'état, les acteurs opérationnels de l'influence produisent leur propre renseignement et leur propre analyse, ce qui leur permet certes d'exploiter ces derniers « en boucle courte », mais limite aussi leurs possibilités.

Sur le plan défensif, la Direction du renseignement militaire (DRM) participe en revanche aux missions de *fact checking* pour endiguer la diffusion de fausses informations d'intérêt militaires, voire pour contrer les tentatives d'intoxication. Cette mission est vouée à gagner en importance dans les années à venir et aurait à impliquer davantage la Direction du renseignement et de la sécurité de la défense (DRSD), dès lors qu'elle contribuera à la protection de la force en opération et sur le territoire national. Cette fonction pourrait à terme être systématiquement intégrée au niveau opératif, à travers la mise en place de cellules de contre-influence au sein même des états-majors déployés.

De même, il apparaît à la lumière des opérations conduites par les acteurs américains, russes et chinois qu'il existe un lien étroit, sinon indissociable entre la lutte informatique offensive (et la collecte de renseignement technique d'origine cyber) et l'exploitation informationnelle, l'exemple le plus criant étant celui des opérations dites de « *hack and leak* ». Inversement, l'expérience de ces dernières années a aussi démontré le rôle de l'influence *en appui* de la LIO, par exemple pour permettre une intrusion.

Les méthodes de *phishing* complexes employées dans de nombreuses campagnes de LIO – à l'instar de *Glowing Symphony* – sont en soi des opérations de déception dont l'objectif est la pénétration technique d'un système d'information. Le rôle prééminent du COMCYBER dans le schéma institutionnel de la LIC s'en trouve ainsi logiquement renforcé mais pourrait sans doute être poussé plus avant dans la comitologie.

Enfin, un dernier enjeu lié à la revalorisation de l'influence en général et de la cyber-influence en particulier tient à la manœuvre en ressources humaines (RH) spécifique qui lui est associée. Les besoins RH en matière d'influence ont toujours été assez distincts de ceux du reste des forces avec une forte prééminence des profils ayant suivi des formations avancées en sciences humaines et sociales (science politique, sociologie, psychologie, langues rares, etc.). L'avènement de la cyber-influence complexifie encore ce profil en ajoutant des besoins en compétences techniques (développeurs, administrateurs systèmes) et, à la charnière des deux, en matière de *data science* (fouille de données, visualisation, apprentissage automatique, marketing digital, *nudge marketing* etc.). Ces profils rares (et chers) posent la question de la capacité des armées à recruter ces compétences, à les faire travailler ensemble (trinômes) et du statut le plus adapté pour ces profils, entre les officiers spécialistes, les officiers sur titre et les contractuels civils.

Associer le secteur privé et la société civile

Les trois grandes puissances dominant aujourd'hui le champ de la cyber-influence font un usage marqué des partenariats publics-privés et du lien avec la société civile, n'hésitant pas à déléguer certaines fonctions à des entreprises ou à orchestrer l'action de certains militants et hacktivistes. Au regard de la nature du cyberespace, de la place de la personnalisation et du débat d'idées, de sa réactivité et de son évolution permanente, le recours à des acteurs issus de la société civile, ne souffrant pas des mêmes contraintes bureaucratiques, juridiques et éthiques semble effectivement nécessaire au développement d'un appareil complet de lutte informationnelle.

À bien des égards, le monde de l'entreprise a aujourd'hui intégré tous les codes de la cyber-influence de façon bien plus systématique et poussé que les armées. Tout comme la propagande des années 1930 s'était inspirée des premières techniques de publicité commerciale, c'est d'abord à des fins de « web marketing » qu'ont été développées les interfaces de programmation applicative (API) permettant de cibler certaines audiences dans le cadre de campagnes d'influence. De même, les actions de déstabilisation de concurrents sont devenues monnaie courante, dans les cadres d'opérations de fusion-acquisition

par exemple – une attaque informationnelle permettant de déprécier la valeur d'un actif que l'on cherche à acquérir. Les acteurs du monde de la communication et de la « veille réputationnelle » tendent ainsi à converger de plus en plus avec ceux de l'intelligence économique. C'est dans ce domaine que sont vraisemblablement forgées aujourd'hui les armes de cyber-influence stratégique de demain. Tout appareil de sécurité informationnel se doit donc de prendre en compte cette dimension pour mieux anticiper les enjeux futurs.

La France n'est pas dépourvue d'acteurs du secteur privé impliqués dans la lutte informationnelle dans le cyberespace (dans les domaines de la recherche, des *think tanks*, du marketing digital, de l'intelligence économique, etc.). Le groupe Avisa Partners né en 2010 et initialement spécialisé dans la communication digitale s'est élargi depuis 2018 à d'autres acteurs issus du monde du *lobbying*, de la sécurité informatique et de l'intelligence économique (à travers l'acquisition en 2020 de la CEIS), attestant de l'existence d'un marché et du besoin de voir émerger un champion français en la matière. Si une telle option doit être considérée avec intérêt, elle doit aussi inciter à la prudence quant au cadre juridique et aux engagements éthiques des partenaires.

Par-delà le recours au secteur privé à des fins de délégation ou de sous-traitance de certaines activités, l'expérience des dix dernières années dans le champ de la cyber-influence a montré l'importance primordiale de disposer de relais solides au sein de la société civile, autrement que par des liens mercantiles et contractuels. La résilience, dans les rues et sur le web, de la société française au lendemain des attentats de l'année 2015 doit nous montrer le chemin. En effet, à la lutte contre la radicalisation sur Internet orchestrée par le Service d'information du gouvernement dans le cadre de la campagne #StopDjihadisme, se sont joint des groupes de « hackeurs éthiques » impliqués dans le contre-discours et la lutte contre l'apologie du terrorisme, le prosélytisme extrémiste et les discours de haine. La création en 2016 de la réserve citoyenne de cyberdéfense s'inscrit également dans cette logique. Sans priver ces acteurs de leur indépendance et de leur spontanéité, il pourrait sembler opportun de raviver cette dynamique, par le biais de formations et de sensibilisation à des menaces autres que le terrorisme en vue d'accroître la résilience de la société dans son ensemble.

Conclusion

L'environnement informationnel a fondamentalement évolué à la faveur de l'apparition des nouvelles technologies numériques et tend désormais à converger avec le cyberespace. Cependant, l'émergence d'une « info-sphère » presque intégralement digitalisée n'a pas simplement donné lieu à un nouveau vecteur des opérations d'influence. Le caractère englobant de ce milieu, ainsi que ses caractéristiques techniques et sociales ont foncièrement modifié la nature de la stratégie militaire d'influence et des opérations d'information qui en découlent. Les grandes puissances comme les acteurs non étatiques les plus virulents l'ont parfaitement compris, s'emparant de ces nouveaux outils pour promouvoir leurs intérêts dans les champs immatériels.

Parmi les cas étudiés – États-Unis, Russie, Chine, mouvance djihadiste – tous démontrent un effort accru pour s'adapter aux caractéristiques du cyberespace et tirer tous les bénéfices de sa vitesse, sa viralité, sa plasticité et son opacité. Tous semblent avoir pris en compte la nécessité d'intégrer autant que possible les champs militaires, du renseignement, de la politique, de l'économique et du social, ainsi que d'assumer un certain écrasement des niveaux tactique, opératif et politico-stratégique. Cette intégration s'est montrée particulièrement prégnante chez les acteurs issus de régimes autoritaires ou de projets extrémistes lesquels semblent « nativement » brouiller les limites entre les différentes catégories. C'est évidemment le cas de la mouvance djihadiste qui lie étroitement l'action informationnelle et l'action militaire. Avec des moyens bien supérieurs, un appareil bureaucratique établi et une maîtrise technologique plus avancée, la stratégie russe s'est caractérisée par son agressivité et sa clandestinité, dont témoigne l'usage bien connu d'usines à *trolls* et de groupes de pirates informatiques. Quant à la Chine, la nature même du régime place la propagande au cœur de son appareil et de son projet politique : le cyberespace n'est que l'extension d'une réalité institutionnelle déjà ancienne. Pékin mise sur la lutte informationnelle et la cyber-influence non seulement pour s'assurer le contrôle accru d'un cyberespace souverain mais aussi pour imposer ses idées à l'étranger.

Inversement, les démocraties libérales semblent éprouver davantage de difficultés face au mélange des genres, au brouillage des catégories et à l'écrasement des niveaux suscités par la cyber-influence. Les États-Unis ont cependant eux aussi adopté l'idée d'une convergence cyber-

informationnelle, *via* la coordination entre le Département d'État et les organes militaires en charge de la cyberdéfense et de la stratégie militaire d'influence. Les progrès rapides de l'intelligence artificielle, des techniques de personnalisation et de modification des contenus, ou les espoirs suscités par la *blockchain* représentent autant de briques technologiques qui transforment la manière dont les armées appréhendent la lutte informationnelle. Le rythme effréné des évolutions du cyberespace et de l'info-sphère laisse augurer de nouveaux usages et de nouvelles techniques de la cyber-influence.

Pour faire face à cette compétition stratégique informationnelle et s'adapter à ce nouveau domaine de lutte, qui les dépasse dans une large mesure, les armées françaises et l'appareil de défense et de sécurité national dans son ensemble doivent donc évoluer, tant sur le plan doctrinal qu'organisationnel. À l'heure où la compétition stratégique s'annonce de plus en plus virulente dans un monde où le multilatéralisme et les mécanismes de coopération internationaux semblent enrayés, un pays ayant l'ambition de conserver son autonomie stratégique ne saurait faire l'économie d'une prise en compte au niveau politique de ce nouvel enjeu. En faisant émerger une chaîne de communication stratégique intégrée à l'échelon ministériel, sous une direction politique responsable, ainsi qu'en revalorisant la place de l'influence dans les armées, et en intégrant davantage le secteur privé et la société civile, la France sera mieux armée pour faire face à ces défis inédits. « *Affluence means influence*[133] » écrivait le romancier américain Jack London en 1905 : cet aphorisme ne semble jamais s'être autant vérifié qu'aujourd'hui.

133. J. London, *War of the Classes*, New York, The Regent Press, 1905.

Institut français
des relations
internationales