diploweb.com La revue géopolitique
ISSN : 2111-4307

La guerre de l'information cherche à accélérer la décomposition des sociétés démocratiques. Entretien avec D. Colon

dimanche 14 janvier 2024,par David COLON, Pierre VERLUISE

Citer cet article / To cite this version :
David COLON, Pierre VERLUISE, **La guerre de l'information cherche à accélérer la décomposition des sociétés démocratiques. Entretien avec D. Colon**, *Diploweb.com : la revue géopolitique, 14 janvier 2024.*

Comment définir la guerre de l'information ? Comment les adversaires des Etats-Unis, notamment l'Iran, la Chine, la Russie ont-ils réagi à la guerre de l'information conduite par les Etats-Unis ? Quelles sont les fonctions des agences de presse et des médias sociaux dans la guerre de l'information contemporaine ? Que font les Etats-Unis mais aussi les États membres de l'UE pour se prémunir de la guerre de l'information conduite par la Russie mais aussi la Chine ?

Voici un entretien majeur avec l'auteur d'un des meilleurs ouvrages publiés depuis trente ans sur la désinformation, enjeu majeur des temps présents et futurs. Vous allez connaitre les grands moments et les principaux acteurs d'une guerre à laquelle nous n'étions pas préparés, devenue menace mortelle pour nos démocraties.

David Colon, auteur de « *La guerre de l'information. Les États à la conquête de nos esprits* », Ed. Tallandier, répond aux questions de Pierre Verluise pour *Diploweb.com*. Avec en bonus la vidéo d'une conférence de D. Colon accompagnée de sa synthèse validée.

Pierre Verluise (P. V.) : Comment pourriez-vous définir la guerre de l'information ?

David Colon (D. C.) : La guerre de l'information désigne au sens strict le fait pour un État de recourir à l'information comme à une arme, à des fins militaires, politiques, économiques, culturelles ou diplomatiques. Elle repose sur l'usage de l'information non seulement comme une source de pouvoir, mais comme un pouvoir en soi, autrement dit comme **un levier de puissance dans les relations internationales**. Au sens large, la guerre de l'information correspond à la « guerre politique » telle que la définissait George Kennan (1904-2005), à savoir « l'emploi de tous les moyens à disposition d'une nation, en dehors de la guerre, pour atteindre ses objectifs nationaux ». Les États recourent ainsi à l'arme informationnelle pour **projeter par-delà leurs frontières leur pouvoir coercitif sans recourir à la force**. La guerre de l'information est, selon une formule de Jiang Zemin en 1993, une « guerre sans fumée ».

P. V. : Alors que l'URSS était un acteur majeur de la guerre de l'information, ce sont pour vous les Etats-Unis qui lors une Guerre froide finissante - dans le contexte de la guerre du Golfe (1990-1991) - ouvrent un nouveau chapitre de la guerre de l'information. De quelles façons ?

D. C. : Les Etats-Unis considèrent être sortis vainqueurs de la Guerre froide et affirment leur suprématie tant militaire que technologique à l'occasion de la Guerre du Golfe. Leur supériorité informationnelle s'exprime d'abord sur le champ de bataille, à travers le recours à la guerre électronique et l'application de la doctrine de la domination informationnelle (*Information Dominance*) consistant pour le Pentagone à faire prévaloir sa supériorité dans le domaine de l'information tout en déniant cette capacité à l'adversaire. Mais cette supériorité s'exprime également dans le champ médiatique, à travers le poids considérable de leurs agences de presses, de leurs médias - et en particulier la chaîne d'information en continu *CNN* - dans la fabrique de l'information médiatique mondiale. Au début de l'ère numérique, leur avance en matière de technologies de l'information et de la communication est telle que les Etats-Unis entendent en faire le fondement d'une domination globale en matière d'information

(*Globale Information Dominance*). A partir de 1990, le principe de libre circulation de l'information et de la communication (*Free flow of Information*), est mis au service de la domination américaine sur l'information mondiale et de la diffusion du modèle démocratique et libéral.

David Colon
David Colon, professeur à Sciences Po Paris, auteur de « La Guerre de l'information. Les États à la conquête de nos esprits », éd. Tallandier, 2023. Photo : David Atlan

P. V. : Comment les adversaires des Etats-Unis, notamment l'Iran, la Chine, la Russie ont-ils réagi à la guerre de l'information conduite par les Etats-Unis ?

D. C. : La Guerre du Golfe et l'effondrement de l'URSS (1991) ont été un choc pour les dirigeants iraniens et chinois, qui ont perçu la supériorité américaine dans le champ informationnel comme **une menace existentielle pour leur régime**. Avant même 2001, la Russie, la Chine et l'Iran se considéraient ainsi en guerre pour la survie de leur régime respectif.

Le choc a été particulièrement fort en Chine, où les dirigeants conservateurs du Parti Communiste avaient vu la main de la CIA dans le printemps de Pékin en 1989 et considéraient que la fin du Parti communiste soviétique était la conséquence d'une ingérence informationnelle américaine. Dès 1993, Jiang Zemin impose par conséquent une posture défensive, consistant à tenir à distance des citoyens chinois les médias occidentaux, à renforcer les moyens de contrôle de l'information en Chine, puis à développer ce que l'on appelle le « Grand pare-feu de Chine », une muraille numérique.

En Russie, la résistance la plus forte à l'encontre de l'hégémonie informationnelle américaine s'est exprimée parmi les *Siloviki*, les hommes du renseignement. En effet, si l'URSS et le Parti communiste d'Union soviétique se sont effondrés, cela n'a pas été le cas des services de renseignement russes. Le renseignement militaire (GRU) s'est maintenu, de même que le KGB divisé désormais entre le FSB (sécurité intérieure, contre-espionnage, collecte de données électromagnétiques) et le SVR (renseignement extérieur). Ils ont poursuivi leurs actions, avec le même ennemi principal, les Etats-Unis, la même doctrine et les mêmes buts. Lorsque Vladimir Poutine, issu du KGB, prend la tête du FSB en 1998, il étend le contrôle de l'Internet russophone, avant de faire adopter une fois parvenu au pouvoir une doctrine de sécurité informationnelle défensive, qui pointe une liste de menaces, dont la « manipulation de l'information » et « le désir de certains pays de dominer et de porter atteinte aux intérêts de la

Russie dans l'espace mondial de l'information ».

P. V. : Comment les États alliés des Etats-Unis ont-ils réagi à la guerre de l'information conduite par les Etats-Unis, puis par les adversaires de Washington D. C. ? Quelles ont été les parts de convergences, divergences, concurrences et coopération ? Pour le dire plus brutalement, les États alliés des Etats-Unis ont-ils été des « idiots utiles », à tout le moins « lents à la compréhension » ?

D. C. : En réalité, les Etats-Unis eux-mêmes ont tardé à réaliser que les régimes autoritaires leur menaient une guerre informationnelle. Ils n'ont prêté attention ni aux premières cyberattaques russes et chinoises, ni à la construction d'un écosystème informationnel mondial reposant à la fois sur des médias internationaux d'État diffusés dans de nombreuses langues, et encore moins à l'essor à bas bruit de l'appareil de renseignement chinois. La raison essentielle est qu'il ne suffit pas, selon la formule de Péguy, de dire ce que l'on voit. **Encore faut-il voir ce que l'on voit**. Or, tout ce que les dirigeants des régimes démocratiques ont voulu voir dans les années 1990 et 2000, c'est la promesse d'une démocratisation et d'une libéralisation de la Chine et de la Russie portée par leur réintégration dans le concert des nations et la conclusion de nombreux accords d'échanges. Ce n'est qu'à partir de 2014 que le Département d'État des Etats-Unis prend réellement conscience de la guerre informationnelle menée par la Russie et la Chine.

En France, la prise de conscience des dirigeants politiques se produit en 2017. Entre temps, **les services de renseignement russes et chinois ont exploité à leur profit cette conviction des régimes occidentaux que la multiplication des échanges économiques et culturels encouragerait la transition démocratique**. Le FSB et le Ministère de la sécurité d'État (MSS) chinois ont pu instrumentaliser ces échanges pour pénétrer en profondeur les sociétés occidentales, capter une partie de leurs élites, constituer patiemment des réseaux d'espionnage et d'influence, et mener à bas bruit une guerre médiatique à force d'achat de pages de publi-reportages et de corruption du débat public par des opérations d'influence plus ou moins clandestines.

> La guerre de l'information d'aujourd'hui, c'est influencer et conditionner les perceptions, insérer des narratifs dans la chaîne de production de l'information de la société adverse.

P. V. : Quelles sont les fonctions des agences de presse et des médias sociaux dans la guerre de l'information contemporaine ?

D. C. : Les médias sont le principal champ de bataille de la guerre mondiale de l'information. Même les opérations numériques les plus sophistiquées aujourd'hui visent souvent d'abord et avant tout à produire des effets dans les médias traditionnels. L'enjeu de cette bataille est l'opinion publique, dont il s'agit d'**influencer et conditionner les perceptions**. Les États influencent la production médiatique à l'extérieur de leurs frontières, d'une part, en recourant à la communication stratégique et la diplomatie publique, et d'autre part à travers l'action clandestine de leurs services de renseignement qui s'emploient à **insérer des narratifs dans la chaîne de production de l'information de la société adverse**. Mais cette bataille pour

les opinions publiques est **asymétrique**, car il est très difficile pour les régimes démocratiques d'influencer les médias des régimes autoritaires, étroitement contrôlés et surveillés, tandis qu'il est particulièrement aisé pour les dictatures d'influencer des sociétés ouvertes, dont les médias sont libres et dont le marché informationnel est aisément accessible par l'entremise de l'achat de médias, de la corruption de journalistes ou plus simplement encore de l'exploitation des caractéristiques mêmes du travail journalistique. « Les médias occidentaux, témoignait en 1994 l'ancien grand maître espion soviétique Pavel Sudoplatov, sont assez facilement manipulables, car ils rédigent souvent leurs articles à partir de communiqués de presse et ont tendance, dans l'ensemble, à ne pas faire de distinction quant à la nature et à la fiabilité de leurs sources ». Ces dernières décennies, la fragilisation croissante des médias occidentaux, soumis à des impératifs de rentabilité dans un contexte de fragilisation de leur modèle économique les a rendus plus perméables que jamais aux influences informationnelles étrangères.

P. V. : Quels sont les comportements spécifiques de la Russie post-soviétique en matière de guerre de l'information ? Vous écrivez que Moscou met en œuvre une « stratégie du chaos en Europe », en partie responsable du Brexit. Par quels moyens, à quelle fin ? De l'autre côté de l'Atlantique, comment l'ingérence russe dans la campagne présidentielle américaine de 2016 a-t-elle été mise en œuvre et à quelle fin ?

D. C. : La spécificité de la Russie est l'application à la sphère informationnelle de « l'art opératif », que l'on peut définir comme une démarche multidimensionnelle qui traduit en objectifs militaires opérationnels la stratégie définie au plus haut niveau par le pouvoir politique. De la sorte, chaque combat tactique revêt une ampleur stratégique et implique toutes les parties prenantes de la guerre de l'information (communication stratégique du Kremlin, diplomatie publique, médias internationaux, fermes de trolls, services de renseignement, agents d'influence…), sans qu'une coordination planifiée de leur action soit toujours nécessaire. **Lorsqu'une opportunité d'action d'influence se présente, chaque acteur russe de la guerre de l'information sait ce qu'il a à faire**.

> Le jour où tout a basculé, selon moi, est le 5 décembre 2011. Voici pourquoi.

La stratégie du Kremlin, d'abord défensive, est devenue offensive dans les années 2000 à la suite des « révolutions de couleur », dans lesquelles les services de renseignement russes ont vu la main de leurs homologues américains, et plus encore des « révolutions twitter » du Printemps arabe, perçus par Vladimir Poutine comme une menace directe de renversement de son régime politique. **Le jour où tout a basculé, selon moi, est le 5 décembre 2011**, lorsque la secrétaire d'État Hillary Clinton dénonce publiquement des « fraudes et des manipulations électorales » à l'occasion des élections législatives russes qui ont vu le parti de Vladimir Poutine, alors Premier Ministre, l'emporter d'une courte tête. Des manifestations ont lieu à Moscou, organisées sur les réseaux sociaux, notamment Facebook. La réaction de Poutine ne se fait pas attendre : aussitôt réélu pour un 3e mandat présidentiel, au printemps 2012, il entreprend de contrôler étroitement l'espace informationnel russe, qu'il ferme progressivement à ceux qu'il dénonce comme des « agents de l'étranger ». Puis il lance une

offensive informationnelle de grande ampleur contre « l'ennemi principal », les Etats-Unis et ses alliés. Tous les moyens publics et privés de la Russie sont alors mobilisés dans le but **d'accélérer la « décomposition » des sociétés démocratiques**, en y encourageant les dissensions préexistantes et le chaos, en y amplifiant la défiance envers les institutions établies, et en y fragilisant le « régime de vérité », c'est-à-dire le cadre d'énonciation de ce qui est vrai et ce qui est faux, dans le but de priver les citoyens occidentaux et leurs dirigeants de la capacité de prendre des décisions rationnelles. Il faut bien comprendre que le but ultime n'était pas tant de parvenir au Brexit ou à l'élection de Donald Trump – objectifs opportunistes à court terme – que de **fragiliser la confiance des citoyens dans leurs dirigeants et dans le processus électoral lui-même**. S'il ne fait plus guère de doute par exemple que le Kremlin a fortement contribué à l'élection de Trump, il est ainsi frappant de constater que 4 jours à peine après son élection, **les organes de propagande du Kremlin organisent à Manhattan des manifestations pour… et contre Trump**. De même, lors des #MacronLeaks en 2017, l'effort principal du Kremlin n'a pas tant été porté sur le soutien à Marine Le Pen que sur la contestation de la légitimité du président élu, Emmanuel Macron. **La fabrique de la défiance et du doute est un travail de longue haleine**, poursuivi par le KGB depuis les années 1950, mais qui a soudain été accéléré par les possibilités offertes par les réseaux sociaux, à commencer par Facebook et Twitter, en matière d'amplification et de propagation des contenus et de ciblage des individus les plus vulnérables psychologiquement.

P. V. : Que font les Etats-Unis mais aussi les États membres de l'UE pour se prémunir de la guerre de l'information conduite par la Russie mais aussi la Chine ? Sommes-nous à la hauteur des enjeux ? Quel est le sort des agents d'influence russe en France ? A vous lire le lecteur peut avoir l'impression qu'après avoir ouvert un nouveau chapitre de la guerre de l'information durant la guerre du Golfe (1990) les Etats-Unis ont été dépassés par les effets boomerang mis en œuvre par leurs compétiteurs. Et que les membres de l'UE n'ont pas compris grand-chose. Pourtant, la désinformation est une « arme de déstabilisation massive ». Que peuvent faire les démocraties face aux menaces hybrides ?

D. C. : Les Etats-Unis ont indubitablement une lourde responsabilité dans la situation de guerre informationnelle mondiale que nous connaissons aujourd'hui. **Ils ont ouvert à trois reprises au moins la boîte de pandore** : en **1991** en prétendant imposer au monde leur domination informationnelle et leur modèle politique, en **2003** en recourant à la manipulation des masses pour légitimer une action militaire menée en-dehors du cadre de l'ONU et visant à renverser le régime de Saddam Hussein, et en **2009** en lançant une cyberattaque destructrice contre les centrifugeuses iraniennes de l'usine de Natanz. A propos de cette dernière opération (appelée « Jeux Olympiques »), le général Michal Hayden, qui avait dirigé successivement la NSA et la CIA, avait exprimé publiquement les craintes que lui inspirait la course aux armements cyber : « **Quelqu'un a franchi le Rubicon** », avait-il déclaré. Comment espérer que les régimes autoritaires se conforment au droit international si vous, régime démocratique, le violez ouvertement ? Comment imaginer qu'ils renoncent à la conquête des esprits de vos citoyens si vous chercher à influencer les leurs ? Comment, enfin, imaginer qu'un virus informatique comme Stuxnet, une fois implanté sur des ordinateurs, puisse un jour, tel le génie, retourner dans sa boîte ?

La prise de conscience, tardive, de l'offensive de la Russie, a conduit en mars 2016 à la création du Centre d'engagement global (*Global Engagement Center*, GEC), un organisme

rattaché au Département d'État mais composé en majorité de personnels du Pentagone et associant des acteurs non étatiques, à commencer par géants américains du numérique, à des actions de contre-influence. Privé de moyens par Donald Trump, le GEC n'a pu véritablement entreprendre de contrer les ingérences informationnelles russes et chinoises qu'à partir de 2020.

Ce n'est qu'en 2018 que l'Union européenne se dote d'un plan d'action contre la désinformation, dans lequel elle définit les « menaces hybrides » comme « le mélange d'activités coercitives et subversives, de méthodes conventionnelles et non conventionnelles [...] susceptibles d'être utilisées de façon coordonnée par des acteurs étatiques et non étatiques [...] sans que le seuil d'une guerre déclarée officiellement soit dépassé ». Toutefois, la seule mesure concrète prise alors par la Commission européenne pour y faire face est la publication, en juillet 2018, d'un « code de bonnes pratiques contre la désinformation », signé par plusieurs plateformes numériques américaines mais qui n'a pas produit les effets escomptés. De même, on peut craindre aujourd'hui que le règlement sur les services numériques (DSA pour *Digital Services Act*, 19 octobre 2022) ne produise pas davantage d'effets sur des acteurs non-coopératifs comme Twitter ou TikTok.

P. V. : Comment la cyberguerre devient-elle chaque jour un champ majeur des États dans la guerre de l'information, éventuellement en synergie ou concurrence avec de grandes entreprises ? Que nous apprend la guerre russe en Ukraine à ce sujet, notamment de l'échec de la cyber offensive russe ?

D. C. : La cyberguerre est mondiale depuis une dizaine d'années, c'est-à-dire depuis que l'Iran, la Russie, la Corée du Nord et la Chine se sont lancés dans des opérations offensives à grande échelle contre les Etats-Unis et leurs alliés. Dans ces États autoritaires, la distinction entre les opérations étatiques et celles émanant de cybercriminels est délibérément brouillée, pour rendre difficile l'attribution des attaques et renforcer le déni plausible des États. Dans cette cyberguerre mondiale, les Etats-Unis disposent pour quelques temps encore une supériorité technologique, sur laquelle ils s'appuient pour proposer à leurs alliés un **« parapluie cyber », qui équivaut en quelque sorte au « parapluie nucléaire »** de la Guerre froide. Concrètement, en Ukraine, cela s'est traduit dès février 2022 par un appui opérationnel non seulement du *Cybercommand* et de la NSA mais également de géants américains du numérique, à commencer par Google et Microsoft, qui ont soutenu le gouvernement ukrainien en l'aidant à faire face aux cyberattaques et en protégeant ses données stratégiques. « Le front russo-ukrainien passe en fait par Redmond [Siège de Microsoft dans l'État de Washington] », déclare bravache Brad Smith, le président de Microsoft. En 2022, les cybercombattants russes se sont trouvés dans la situation inédite de devoir mener à la fois des actions offensives contre l'Ukraine, des actions défensives face aux cyberattaques des hackers ukrainiens et de leurs alliés, et une cyberguerre mondiale contre la NSA. Cela explique en grande partie le fait que la cyberoffensive russe n'ait pas produit d'effets significatifs, contrairement à ce qui s'était produit en 2014 lors de l'annexion de la Crimée.

> Début 2024, il nous manque encore une stratégie nationale de lutte contre les manipulations étrangères de l'information.

P. V. : 2024 sera une année électorale dans bien des pays. Dans le cas de l'UE les

élections pour le Parlement européen sont un enjeu pour les citoyens … comme pour les États extra-européens qui entendent torpiller de l'intérieur l'UE. Existe-t-il des structures de lutte contre les ingérences étrangères dans les processus électoraux français et des pays de l'UE ?

D. C. : La France s'est dotée en 2017 du Commandement Cyber (Combcyber), chargé de la lutte informatique défensive (LID), offensive (LIO) et d'influence (L2I), en 2021 de Viginum, un service chargé de la vigilance et de la protection contre les ingérences numériques étrangères, et en 2022 une sous-direction de la veille et de la stratégie au sein du Ministère des affaires étrangères. Cette même année, le Président de la République a élevé l'influence au rang de nouvelle fonction stratégique. Depuis-lors, la France a remporté quelques batailles dans la guerre informationnelle contre la Russie, comme en 2022, lorsque le porte-parole de l'armée le colonel Pascal Ianni a mis en échec une opération de manipulation de l'information à Gossi, au Mali ; ou en 2023, lorsque Viginum a permis de dévoiler et de déjouer en partie les opérations de désinformation du réseau dit « Doppelgänger/RRN ». Toutefois, à ce jour **il nous manque encore une stratégie nationale de lutte contre les manipulations**, tandis que les organismes existants, à commencer par Viginum, manquent encore de moyens et d'effectifs pour être en mesure faire face à la menace à l'approche des élections européennes et des Jeux Olympiques de Paris 2024, dans le contexte d'une part de l'alliance entre la Chine, la Russie et l'Iran et d'autre part de l'essor de l'Intelligence artificielle.

> Quel est l'objectif à court terme ? Et quel est l'objectif à long terme ? Réponses.

Depuis 2020, le Parti communiste chinois a ainsi intensifié sans retenue ses opérations offensives, en suivant pas à pas l'exemple russe. A la différence de la menace russe, très peu discrète, **la menace chinoise s'exprime à bas-bruit, et repose notamment sur une reconfiguration patiente de l'écosystème informationnel mondial**, à travers la diffusion de ses propres médias, des accords de partenariat avec des médias locaux, par exemple africains, et le recrutement massif d'influenceurs tant numériques que politiques dans les États démocratiques. La Chine, dès 1993, avait été le premier État autocratique à se réapproprier le concept de *Soft Power* (*ruan shili).* Depuis 2013 et l'arrivée au pouvoir de Xi Jinping, elle est passée maître dans l'art du *Sharp Power*, la « Puissance tranchante », qui désigne la politique manipulatrice des régimes autoritaires qui pénètrent et perforent les environnements politiques et informationnels des États démocratiques dans le but d'influencer et de saper leur système politique. Au même titre que la Russie, la Chine est désormais un acteur majeur des ingérences informationnelles et des interférences dans les processus électoraux. En Europe, dans le cadre des élections de 2024, le Parti communiste chinois s'emploie avant tout à fragiliser l'alliance entre les pays européens et les Etats-Unis, qui demeurent leur cible principale, dans la perspective de l'élection présidentielle américaine de novembre 2024.

Depuis 2022, on constate une convergence croissante non seulement des modes d'action mais des infrastructures et des contenus entre l'écosystème informationnel russe, chinois et iranien. L'objectif à court terme est **d'affaiblir les États démocratiques, l'objectif à long terme est de substituer à l'hégémonie informationnelle occidentale une hégémonie informationnelle de l'Axe Moscou-Téhéran-Pékin**. Ce qui rend cet objectif atteignable est

d’une part la puissance économique, financière et industrielle de la Chine, et d’autre part le recours croissant à l’Intelligence artificielle, aussi bien pour produire massivement de faux contenus, de faux profils et de faux médias difficilement détectables que pour amplifier massivement la propagation de la désinformation et pour détecter automatiquement des failles tant dans les systèmes d’information numériques que dans les esprits des utilisateurs de réseaux sociaux. L’ampleur, la gravité et l’immédiateté de la menace informationnelle représentée par l’IA est tout à fait inédite.

Bonus vidéo. David Colon. Comment les États mettent-ils en œuvre la guerre de l’information ?

Cette vidéo peut être diffusée en amphi pour nourrir un cours et un débat. Voir la synthèse par Marie-Caroline Reynier pour Diploweb.com, relue et validée par David Colon. Voir la vidéo sur youtube/Diploweb

---

P. V. : La publication de votre excellent ouvrage, « La Guerre de l’information. Les États à la conquête de nos esprits », éd. Tallandier, a reçu un très bel accueil du public mais aussi de certains cercles dirigeants. Est-il possible d’espérer des évolutions constructives et pérennes à la hauteur des enjeux ?

D. C. : Je voulais à travers ce livre, à la fois alerter l’opinion, armer les esprits et proposer des pistes pour faire face à la guerre de l’information tout en préservant les principes fondamentaux de la démocratie libérale. L’accueil que le livre a reçu, notamment auprès des élus et des acteurs français, civils et militaires, de la lutte informationnelle d’influence, a dépassé toutes mes espérances. Si le livre a pu contribuer à une prise de conscience de l’enjeu majeur que constitue la guerre de l’information, j’en suis ravi. Désormais, je m’emploie dans mes recherches comme dans mon action à promouvoir des solutions concrètes pour protéger nos esprits en même temps que nos libertés fondamentales.

Plus

. David Colon, *La guerre de l’information. Les États à la conquête de nos esprits* . Ed. Tallandier, 476 p.

4e de couverture

Une guerre à laquelle nous n'étions pas préparés se déroule sous nos yeux, pour l'essentiel sans que nous en soyons conscients, et constitue pour nos démocraties une menace mortelle. Depuis la fin de la Guerre froide et l'essor d'Internet et de médias planétaires, la militarisation de l'information par les États bouleverse l'ordre géopolitique. La guerre de l'information, qui oppose les États autoritaires aux régimes démocratiques, démultiplie les champs de bataille et fait de chaque citoyen un potentiel soldat. Plus que jamais, la puissance des États –qu'il s'agisse de leur *hard power*, leur *soft power* ou leur *sharp power*– dépend de leur capacité à mettre leurs moyens de communication au service de leur influence, en recourant à la cyberguerre, à la désinformation ou à l'instrumentalisation de théories du complot. À l'ère de l'intelligence artificielle et de la guerre cognitive, les médias sociaux sont le théâtre d'une « guerre du Net » sans merci, sans fin, dont nos esprits sont l'enjeu.

Dans cet ouvrage, David Colon, spécialiste de l'histoire de la propagande et de la manipulation de masse, décrit les mécanismes de cette guerre longtemps restée secrète en dévoilant les stratégies de ses commanditaires et en décrivant les tactiques et le parcours de ses acteurs, qu'ils soient agents secrets, diplomates, journalistes ou hackers.

P.-S.

David Colon, professeur à Sciences Po Paris, auteur de « La Guerre de l'information. Les États à la conquête de nos esprits », éd. Tallandier, 2023. David Colon est chercheur au Centre d'histoire de Sciences Po. Il y enseigne l'histoire de la communication, des médias et de la propagande. Membre du Groupement de recherche « Internet, IA et société » du CNRS. Il a précédemment publié « Propagande » (éd. Belin 2019, rééd. Flammarion, Champs histoire 2021) distingué par les prix Akropolis et Jacques Ellul. Il a aussi récemment publié « Les Maitres de la manipulation », éd. Texto, 2023. D. Colon a rejoint le Conseil scientifique du *Diploweb.com*. Propos recueillis par Pierre Verluise, docteur en Géopolitique, fondateur du *Diploweb.com*