

DAVID  
COLON

La  
**Guerre**  
de  
**l'information**

*Les États à la conquête de nos esprits*



PAR L'AUTEUR DES  
**MAÎTRES DE  
LA MANIPULATION**

Tallandier





LA GUERRE  
DE L'INFORMATION

## DU MÊME AUTEUR

*Propagande. La manipulation de masse dans le monde contemporain*,  
Belin, 2019 ; Flammarion, coll. « Champs histoire », 2021.

*Les Maîtres de la manipulation. Un siècle de persuasion de masse*,  
Tallandier, 2021 ; coll. « Texto », 2023.

*Rupert Murdoch. L'empereur des médias qui manipule le monde*,  
Tallandier, 2022.

David Colon

LA GUERRE  
DE L'INFORMATION

*Les États à la conquête de nos esprits*

TALLANDIER  
*ESSAIS*

© Éditions Tallandier, 2023  
48, rue du Faubourg-Montmartre – 75009 Paris  
[www.tallandier.com](http://www.tallandier.com)  
ISBN : 979-10-210-5588-9

Pour mes filles, Célestine et Augusta



## INTRODUCTION

### La guerre que l'on n'a pas vu venir

Nous étions en guerre, et nous ne le savions pas. Il n'y a pas eu de déclaration de guerre, pas d'appel à la mobilisation, pas de discours guerrier dans les médias, ni d'ennemi désigné. Tout semblait indiquer qu'avec la chute du mur de Berlin et la fin de la guerre froide en 1989, puis l'effondrement de l'URSS en 1991, la démocratie libérale allait triompher, et avec elle l'information libre diffusée par-delà les frontières par des médias de masse. La machine de propagande de la guerre froide, qui avait vu s'opposer deux modèles concurrents, était soudain devenue obsolète. La globalisation des médias, c'est-à-dire la diffusion à l'échelle mondiale de contenus, rendue possible par les nouvelles technologies, portait la promesse d'un accès universel à l'information. Sur un marché désormais libre, les meilleures idées étaient appelées à chasser les mauvaises, et la vérité à supplanter les mensonges. À la « révolution CNN » s'est bientôt superposée celle du Web et des « autoroutes de l'information » qui étaient vouées à saper les derniers États autoritaires de la planète et à encourager l'émancipation des peuples. Les médias de masse étaient partie prenante dans la mondialisation, et devaient contribuer à la paix en rapprochant les cultures et en favorisant la compréhension mutuelle.

Dans le même temps, l'avènement de la télévision par satellite et du Web a bouleversé l'ordre géopolitique et les équilibres de pouvoir, en conférant à l'information une dimension plus stratégique que jamais et en transformant la nature de la puissance. L'information, qui avait toujours été une source de pouvoir, était devenue un pouvoir en soi, un levier de puissance dans les relations internationales. Jusqu'alors, les États avaient été difficilement contournables pour communiquer d'un pays à l'autre : qu'il s'agisse de réguler le trafic des lignes télégraphiques internationales, d'autoriser des télévisions ou des radios à émettre, ou de contrôler, censurer éventuellement, le contenu des communications, l'État était présent partout. Le contrôle des flux d'information a été, avec le monopole de la violence légitime, l'une des caractéristiques majeures des États-nations au XX<sup>e</sup> siècle. Or, les satellites et Internet ont changé cela radicalement, en permettant à des acteurs privés de communiquer à l'échelle internationale sans la médiation de l'État, dont ils ont pu ainsi remettre en cause la souveraineté. En outre, de « petites puissances » et des organisations non gouvernementales (ONG) se sont retrouvées en mesure de contester, par le recours à l'information transnationale, l'hégémonie des grandes puissances, à commencer par celle des États-Unis. Les médias électroniques diffusés par satellite et les moyens de communication sur le Web ont permis aux propagandistes de contourner les barrières physiques, législatives et politiques qui étaient destinées à protéger les populations des ingérences informationnelles étrangères. En outre, de nombreux États ont également entrepris de remettre en cause la supériorité technologique des États-Unis et de leurs alliés dans le domaine de l'information. Les États autoritaires, à commencer par la Chine, ont interprété ces bouleversements comme un risque existentiel, et ont agi en conséquence en protégeant leur espace informationnel des

ingérences étrangères avant de militariser leur information à destination des États démocratiques.

En l'espace de quelques années à peine, la puissance des États en est venue à dépendre comme jamais auparavant de leur capacité à recourir à l'information comme à une arme, à des fins militaires, politiques ou diplomatiques. Sans que les opinions publiques en prennent conscience, les démocraties et les régimes autoritaires se sont ainsi engagés dans une guerre de l'information à l'échelle planétaire, au service de leur puissance, de leur influence internationale, que l'on peut définir comme la capacité à produire un effet sur les conduites des sociétés et des élites de pays étrangers, comme de leur « pouvoir discursif », c'est-à-dire leur capacité à faire valoir leur récit et à maîtriser les discours les concernant sur la scène internationale<sup>1</sup>.

La guerre de l'information, qui était jusqu'alors le plus souvent le prolongement de la guerre ouverte par le recours à des opérations à caractère informationnel, est devenue un substitut à certains conflits militaires. Elle correspond à la définition que le politologue et ancien ambassadeur des États-Unis George Kennan donnait de la « guerre politique » en temps de paix, à savoir « l'emploi de tous les moyens à la disposition d'une nation, en dehors de la guerre, pour atteindre ses objectifs nationaux » : « Ces opérations, écrit Kennan, sont à la fois manifestes et secrètes. Elles vont d'actions manifestes telles que les alliances politiques, les mesures économiques et la propagande "blanche" à des opérations secrètes comme le soutien clandestin d'éléments étrangers "amis" et la guerre psychologique "noire"<sup>2</sup>. » Les États recourent à la « guerre politique » pour projeter leur pouvoir coercitif sans recourir à la force.

À la différence de la guerre conventionnelle, la guerre de l'information n'a ni début ni fin, et brouille les distinctions

traditionnelles entre l'état de guerre et l'état de paix, entre ce qui est officiel et ce qui est secret, entre opérations étatiques et opérations non étatiques, en raison du recours massif et quasi systématique à des sous-traitants, des mercenaires. Souvent, les campagnes informationnelles sont associées à des opérations de guerre irrégulières, dans le cadre de conflits hybrides, qui mêlent dans l'espace de combat des activités conventionnelles, non conventionnelles (diplomatiques, économiques, technologiques), irrégulières, terroristes et criminelles, en restant en deçà du seuil d'une guerre déclarée. Les guerriers de l'information annihilent toute distinction entre le front et l'arrière, et combinent actions létales et manipulations informationnelles non létales, de l'influence à la cyberguerre\* que l'on peut définir comme « l'utilisation des différentes composantes du cyberspace à des fins de contrôle<sup>3</sup> », et qui a pour théâtre d'opérations les réseaux informatiques, en passant par la guerre électronique\*, qui consiste à « exploiter le spectre électromagnétique dans le but de combattre un adversaire ou de s'en protéger<sup>4</sup> ». Les caractéristiques des campagnes informationnelles encouragent de nombreux acteurs à y recourir sans craindre de provoquer un conflit ouvert, de sorte que le champ de ces conflits n'a cessé de s'étendre depuis 1989. À l'équilibre de la guerre froide a succédé le déséquilibre de la guerre de l'information.

Au-delà du champ de la guerre proprement dit, en effet, les opérations informationnelles consistent essentiellement à organiser des campagnes de propagande et de manipulation dans un cadre international pour influencer l'opinion publique d'autres pays. Il s'agit tantôt d'obtenir l'adhésion de populations alliées, tantôt de subvertir ou de déstabiliser l'opinion

---

\* Les mots signalés par un astérisque sont définis dans le glossaire en fin d'ouvrage, p. 455.

publique des ennemis, notamment par le recours à la désinformation\*. De fait, la globalisation des médias a donné un nouvel essor à la diplomatie publique\* qui, à la différence de la diplomatie traditionnelle, d'État à État, désigne, comme l'écrit l'historien Nicholas Cull, « la tentative d'un acteur international de gérer l'environnement international en s'engageant auprès d'un public étranger<sup>5</sup> ». Cette diplomatie d'influence trouve dès les années 1990 de nouveaux et puissants relais dans les médias internationaux et le Web. Les États-Unis, la Russie et la Chine ont réalisé, dès 1991, l'enjeu stratégique que représente désormais l'information. « Un des attributs de la guerre future, écrit ainsi en 1998 Vladimir Slipchenko, théoricien de la transformation des forces armées russes, sera la confrontation de l'information, car l'information est en train de devenir une arme du même type que les missiles, les bombes, les torpilles, etc.<sup>6</sup> »

La guerre de l'information requiert de se doter de capacités d'espionnage et de surveillance électroniques, mais aussi de sécurisation des systèmes d'information et de piratage de ceux de l'adversaire. Le théâtre de ce nouveau type de conflit est la sphère informationnelle, ou infosphère, et ses outils incluent aussi bien les médias traditionnels que les nouvelles technologies de l'information et de la communication, comme Internet et les téléphones mobiles. L'infosphère devient un nouvel espace de conflictualité, qui s'ajoute aux terrains physiques (terre, mer, air, espace) et électromagnétiques. La gestion de l'environnement informationnel est désormais un élément à part entière tant du champ de bataille lui-même que de la conflictualité entre les États : la guerre de l'information est une guerre des perceptions aussi bien que du sens et de l'influence.

Les acteurs principaux de la guerre de l'information sont d'abord les armées et les services de renseignement, qui se sont souvent dotés de systèmes de contrôle conçus pour

accompagner les opérations militaires à toutes les échelles (tactique, opérationnelle, stratégique) et à tous les niveaux. En mars 1992, le général Colin Powell, alors président de l'état-major interarmées des États-Unis, publie un « Mémoire sur la guerre de l'information », qu'il définit comme des opérations visant à « décapiter la structure de commandement de l'ennemi à partir de son corps de forces de combat<sup>7</sup> ». Pour les armées, la guerre de l'information désigne donc l'usage offensif et défensif de l'information pour exploiter, corrompre et détruire les systèmes de l'adversaire, tout en protégeant ses propres informations et systèmes. Il s'agit d'abord d'opérations cyber (*Computer Network Operations*), qui visent à interférer avec l'activité informatique de l'ennemi, au besoin par le recours au sabotage, tout en garantissant à ses propres troupes la meilleure sécurité informationnelle (*Operations Security, OpSec*). Il s'agit ensuite de guerre électronique, consistant à brouiller les communications adverses, et d'intoxication, qui a pour but de tromper l'ennemi sur ses propres intentions. Il s'agit enfin d'opérations psychologiques (*Psychological Operations, PsyOps\**), visant à influencer les opinions, les émotions, les motivations et les comportements des troupes ennemies ou des civils. Il peut s'agir notamment de désinformer, de manipuler, d'introduire le doute, d'induire les services adverses en erreur.

En 1993, John Arquilla et David Ronfeldt, deux politologues de RAND Corporation, un groupe de réflexion proche du Pentagone et spécialisé dans l'analyse stratégique, annoncent dans un article retentissant l'avènement de la « guerre cyber » : « La révolution de l'information, écrivent-ils, entraînera des changements à la fois dans la manière dont les sociétés peuvent entrer en conflit et dans la manière dont leurs forces armées peuvent faire la guerre<sup>8</sup>. » Les deux auteurs distinguent en effet la « guerre du Net » (*Netwar*), c'est-à-dire « les conflits

idéologiques au sein de la société qui se déroulent en partie par le biais de modes de communication sur Internet », en impliquant les médias ou la diplomatie, et la « cyberguerre », dans laquelle des pirates informatiques pourraient cibler à distance des économies et désactiver des capacités militaires. À leurs yeux, les futurs conflits seront gagnés non pas par des forces physiques, mais par la maîtrise et la manipulation de l'information. Plus encore, la « guerre du Net » implique un nouveau type de conflit, dans lequel l'information en ligne elle-même devient une arme. Arquilla et Ronfeldt entrevoient ainsi que des changements massifs, jusqu'alors engendrés par des conflits armés, pourraient être provoqués sans même tirer un seul coup de feu. De fait, à l'ère numérique, l'infosphère se confond en partie avec le cyberspace, qui lui confère une dimension potentiellement universelle et immédiate. Inventé en 1984 par l'écrivain William Gibson, qui y voyait une « représentation graphique de données extraites des mémoires de tous les ordinateurs du système humain », le mot cyberspace désigne depuis un ensemble de données numérisées, lié à l'interconnexion des ordinateurs, des machines et des objets, qui représente un espace parallèle à notre espace physique<sup>9</sup>. Alors qu'il a longtemps cristallisé des espoirs d'émancipation humaine, le cyberspace s'est révélé le théâtre majeur d'une guerre souterraine de l'information, affectant les trois couches qui le composent : la couche physique, celle des équipements et des réseaux ; la couche logique, constituée des protocoles et des logiciels ; et la couche cognitive, celle des informations et des interactions sociales.

Dans les années 1990, la « guerre du Net » n'en est encore qu'à ses balbutiements, mais la cyberguerre est déjà intégrée à la doctrine de la plupart des armées modernes. En effet, le numérique affecte plusieurs composantes des conflits militaires, à commencer par l'espionnage, le sabotage et la désinformation,

qu'elle rend à la fois moins coûteuses et plus simples que les opérations menées par des saboteurs pendant la guerre froide. Il est en outre beaucoup plus difficile d'attribuer une opération de guerre numérique qu'une opération d'espionnage humain. Enfin, le numérique est porteur d'un « pouvoir égalisateur », qui confère aux petites puissances et aux acteurs non étatiques les moyens de s'en prendre à de grands acteurs des relations internationales tout en échappant aux mécanismes de dissuasion traditionnels<sup>10</sup>. Par conséquent, l'utilisation des moyens numériques à des fins de contrôle devient un élément central de la réflexion stratégique et tactique.

Elle l'a particulièrement été dans les régimes autoritaires, qui ont d'abord été soucieux de préserver leur souveraineté et leur stabilité face à l'essor de nouvelles technologies perçues comme des menaces, avant de retourner ces mêmes technologies contre leurs opposants et contre les démocraties libérales. Car les armes de la guerre de l'information, qui ont démultiplié la puissance des États-Unis et de certains de leurs alliés, ont en même temps constitué des vulnérabilités nouvelles que les régimes autoritaires ont prises en compte pour s'en protéger avant de les exploiter dans le but d'affaiblir les démocraties. Dès la fin de la guerre froide, l'hégémonie informationnelle américaine a été activement contestée, tant par des acteurs étatiques que par des acteurs non étatiques qui ont su faire de l'information une arme asymétrique. Dans le même temps, l'espace informationnel a connu une militarisation rampante, à l'initiative des armées et des services de renseignement de plusieurs États qui ont eu recours à l'information pour préparer et parfois mener une guerre qu'ils ne pouvaient pas ou ne voulaient pas mener par des moyens classiques. Depuis plus de trente ans, les démocraties ont été mises à l'épreuve par la guerre de l'information. Engagées dans une course aux armements informationnels,

## INTRODUCTION

elles ont développé des outils d'influence, qui se sont tour à tour retournés contre elles, à l'image des médias sociaux\* : parce que ceux-ci permettent la création et la publication de contenus par leurs utilisateurs ainsi que la mise en relation de ces derniers, ils ont bousculé des régimes autoritaires avant d'être instrumentalisés par eux pour fragiliser les bases des régimes démocratiques.

Les démocraties ont souvent tardé à identifier la menace protéiforme que faisait peser sur elles le recours à la guerre de l'information par des États qui souhaitaient leur perte. « Aujourd'hui, nous sommes tous acteurs d'une guerre mondiale de l'information qui est omniprésente, difficile à comprendre et injuste », constate en 2019 Richard Stengel qui, en tant que sous-secrétaire d'État pour la Diplomatie publique des États-Unis, avait été chargé de contrer la propagande de Daech et de la Russie. « Une guerre, ajoute-t-il, que nous ne savons pas encore très bien comment combattre<sup>11</sup>. » Ce livre raconte l'histoire de cette guerre à laquelle nous n'étions pas préparés, qui s'est déroulée pour l'essentiel sans que nous en soyons conscients, et qui constitue pour nos démocraties une menace mortelle.



## CHAPITRE PREMIER

### La guerre du Golfe, point de départ de la guerre de l'information mondiale

Le 10 octobre 1990 se tient à Washington une session extraordinaire de la Commission des droits de l'homme du Congrès des États-Unis, créée en 1983 par Tom Lantos, un élu démocrate californien survivant de la Shoah, et John Porter, un élu républicain de l'Illinois. Il s'agit, pour ces deux défenseurs des droits humains, de se pencher sur les accusations de crimes de guerre portées contre l'armée irakienne depuis qu'elle a envahi le Koweït, le 2 août précédent. Leur dernier témoin, en ce jour d'octobre, est une jeune fille de 15 ans, identifiée à l'époque par son seul prénom, Nayirah. « Je viens de sortir du Koweït, témoigne-t-elle. Ma mère et moi [y étions] pour des vacances d'été paisibles. Ma sœur aînée a eu un bébé le 29 juillet et nous voulions passer un peu de temps au Koweït avec elle. [...] La deuxième semaine après l'invasion, je me suis portée volontaire à l'hôpital Aldar avec douze autres femmes qui voulaient aussi aider. J'étais la plus jeune volontaire. Les autres femmes avaient entre 20 et 30 ans. Pendant que j'étais là, j'ai vu les soldats irakiens entrer dans l'hôpital avec des fusils. Ils ont sorti les bébés des couveuses, pris les couveuses et laissé les enfants mourir sur le sol froid.

C'était effrayant. » Ce témoignage est diffusé en direct par C-SPAN, la chaîne parlementaire américaine, et en différé sur ABC et NBC, touchant quelque 53 millions d'Américains<sup>1</sup>. Le témoignage bouleversant de Nayirah se retrouve aussitôt à la une de l'actualité américaine et mondiale, et les appels à une intervention militaire se multiplient. Le 29 novembre 1990, le Conseil de sécurité des Nations unies adopte une résolution autorisant le recours à la force contre l'Irak et pose un ultimatum au 15 janvier. Enfin, le 12 janvier 1991, le Congrès des États-Unis autorise à son tour le recours à la force, avec une très courte majorité au Sénat.

### *L'ingérence informationnelle du Koweït aux États-Unis*

Le 10 octobre 1990 est une date clé dans la marche à la guerre, mais il consacre également le déclenchement d'une autre guerre, alors invisible : une guerre de l'information, lancée en secret par le gouvernement en exil du Koweït. À la suite de l'invasion irakienne, ce dernier a engagé une vingtaine d'agences de relations publiques et de cabinets d'avocats dans le but de mobiliser l'opinion publique américaine contre Saddam Hussein. Sous couvert du groupe « Citoyens pour un Koweït libre » (*Citizens for a Free Kuwait*, CFK), le gouvernement koweïtien a ainsi entrepris la plus importante campagne d'influence jamais menée aux États-Unis, avec l'aval tacite de l'administration américaine, qui ne recourt pas aux dispositions de la loi FARA (*Foreign Agent Registration Act*) de 1938 faisant pourtant obligation aux agents étrangers de déclarer leurs activités. La société de relations publiques Hill & Knowlton, recrutée dès le 9 août 1990, est ainsi rémunérée entre 10 et 12 millions de dollars pour influencer l'opinion publique américaine en faveur du Koweït<sup>2</sup>. Elle organise des

## TABLE

INTRODUCTION. – La guerre que l'on n'a pas vu venir...	9
CHAPITRE PREMIER. – La guerre du Golfe, point de départ de la guerre de l'information mondiale.....	19
CHAPITRE 2. – Les États-Unis en quête de domination globale de l'information.....	43
CHAPITRE 3. – Les résistances face à la domination informationnelle américaine.....	63
CHAPITRE 4. – Les médias, champ de bataille de la guerre secrète de l'information.....	97
CHAPITRE 5. – La guerre des boutons de partage sur les médias sociaux.....	125
CHAPITRE 6. – La Russie déclenche la guerre totale de l'information .....	161
CHAPITRE 7. – La cyberguerre mondiale.....	195
CHAPITRE 8. – La guerre contre l'information : la désinformation, arme de déstabilisation massive ...	235
CHAPITRE 9. – La France face à une guerre qu'elle tarde à reconnaître comme telle .....	273
CHAPITRE 10. – Les théories du complot et la guerre psychologique.....	301

## LA GUERRE DE L'INFORMATION

CHAPITRE 11. – L'Ukraine, théâtre de la guerre 3.0 ....	337
CHAPITRE 12. – La Chine et l'avenir de la guerre cognitive .....	371
CONCLUSION. – Pour un état d'urgence informationnel.....	403
NOTES .....	419
GLOSSAIRE.....	455
LISTE DES SIGLES.....	459
BIBLIOGRAPHIE .....	461
INDEX DES NOMS DE PERSONNES .....	469