diploweb.com La revue géopolitique
ISSN : 2111-4307

Vidéo. Comment les États mettent-ils en œuvre la guerre de l'information ? D. Colon

mardi 28 novembre 2023,par Arthur ROBIN, David COLON, Marie-Caroline REYNIER, Pierre VERLUISE

Citer cet article / To cite this version :
Arthur ROBIN, David COLON, Marie-Caroline REYNIER, Pierre VERLUISE, **Vidéo. Comment les États mettent-ils en œuvre la guerre de l'information ? D. Colon**, *Diploweb.com : la revue géopolitique, 28 novembre 2023.*

Comment la guerre de l'information structure-t-elle les relations internationales depuis les années 1990 ? Pourquoi l'avènement de l'ère numérique et de médias internationaux permet-il aux États d'interférer plus directement ? À partir d'un vaste panorama très documenté, David Colon présente clairement les cas des grands acteurs de la guerre de l'information. Des clés pour comprendre.

Cette vidéo peut être diffusée en amphi pour nourrir un cours et un débat. Voir sur youtube/Diploweb

Synthèse par Marie-Caroline Reynier pour Diploweb.com, relue et validée par David Colon

Bien qu'on ne la perçoive pas toujours, la guerre de l'information structure les relations internationales depuis les années 1990. En effet, l'avènement de l'ère numérique et de médias internationaux tels que *CNN* permet désormais aux États d'interférer plus directement. À partir d'un panorama depuis les années 1990 à aujourd'hui, David Colon s'intéresse aux États-Unis, à la Russie et à la Chine comme acteurs de la guerre de l'information. Voici la vidéo et la synthèse d'une conférence organisée par *Diploweb.com* et l'ADEA MRIAE de l'Université Paris I, le 12 octobre 2023, en partenariat avec le Centre géopolitique.

Les États-Unis en quête de domination informationnelle mondiale

D. Colon identifie la guerre du Golfe (2 août 1990 – 28 février 1991) comme point de départ de la guerre de l'information. Les États-Unis y manifestent leur puissance militaire, économique mais utilisent également le recours à l'information comme arme. À travers la doctrine de la « guerre en réseaux » (*Network-Centric Warfare*), ils veulent dominer le champ de l'information. Cette guerre du Golfe est un tournant, précisément car elle est perçue comme telle par la Chine et la Russie.

Par la suite, les États-Unis cherchent à étendre leur domination informationnelle (*Information Domination)* via les « autoroutes de l'information », l'affirmation de leur *soft power* et la création de géants du numérique (Google en 1998 notamment). À cette période, comme le souligne le discours du président B. Clinton devant les étudiants de l'Université de Pékin (1998), les États-Unis pensent que l'extension de leur système informationnel au monde entier conduira les derniers régimes autoritaires à disparaître.

D. Colon relate également à quel point le film *Les experts/Sneakers* (1992), visionné par McConnell, directeur de la *National Security Agency* (NSA), a produit des effets directs sur la politique de défense américaine. Ce film accélère la prise de conscience du basculement dans une nouvelle ère, celle de l'information électronique. Il met en exergue la nécessité de faire évoluer les outils et les méthodes de la NSA, pour favoriser la pénétration des réseaux ennemis. En ce sens, dès 1992, l'agence fédérale américaine chargée de la collecte des données électromagnétiques (SIGINT) redéfinit ses missions pour se lancer à grande échelle dans des opérations de cyberguerre.

Ensuite, la manipulation massive de l'opinion mondiale pour légitimer l'entrée en guerre des États-Unis contre l'Irak en 2003 apparaît comme un deuxième point de rupture. En effet, le recours à la manipulation de l'information mondiale, doublé d'une entorse au droit international n'est pas sans conséquence sur l'attitude des régimes autoritaires.

Enfin, l'utilisation du virus *Stuxnet* par les autorités américaines en 2009-2010 [opération conjointe avec les Israéliens mettant hors d'usage des centrifugeuses de l'usine iranienne d'enrichissement de Natanz] constitue un troisième point de rupture. Pensé comme un moyen de détourner les opérations iraniennes, ce virus, utilisé par la suite par des hackers iraniens, constitue le point de départ d'une cyberguerre mondiale.

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

La riposte russe

Si D. Colon utilise le terme de « riposte », il rappelle que l'action des services de renseignement russes s'inscrit dans la durée. Ainsi, la génération formée à l'art de la désinformation dans les années 1980 est actuellement au pouvoir, au premier rang duquel Vladimir Poutine qui fut agent de liaison du KGB auprès de la Stasi (police politique de la RDA) de 1985 à 1990. Pour les services de renseignement russes, la désinformation ne se définit pas comme l'obtention d'un résultat immédiat mais comme **un lent travail de décomposition de la société adverse**.

La spécificité russe en la matière tient au fait que ses trois services de renseignement et de sécurité réalisent des activités à l'étranger. Ainsi, le FSB (Service fédéral de sécurité) est chargé de la sécurité intérieure mais mène également des activités cyber offensives. D. Colon souligne que l'articulation faite en Russie entre activités de renseignement intérieur et extérieur est inenvisageable aux États-Unis entre le FBI et la NSA. De son côté, le SVR (Service russe des renseignements extérieurs) s'est lancé depuis les années 1990 dans des activités de renseignement sur Internet. Enfin, le GRU (Service de renseignement militaire), créé en 1918, fusionne des capacités de guerre psychologique acquises durant la Guerre froide avec des outils numériques.

La force des services de renseignement russes tient également dans leur appropriation du mode de pensée occidental. Selon les principes définis par N. Wiener, les Russes envisagent un

usage militaire de l'information pour protéger leur sphère informationnelle de l'ennemi. Ils mènent également une guerre de subversion pour conquérir les esprits et semer le chaos partout où ils le peuvent. Leur efficacité tient donc à une conception défensive et offensive du conflit informationnel, tel que défini notamment par I. Panarin et S. Rastorguev.

Parmi les coups d'éclat des services de renseignement russes, la cyberattaque menée en 2007 en Estonie à l'encontre de sites web d'organisations gouvernementales fait date. D. Colon relève que ces opérations cyber sont systématiquement accompagnées d'opérations médiatiques, souvent plus fortes après l'attaque qu'avant. Par exemple, après l'élection de Trump en 2016, les Russes organisent des manifestations en faveur et à l'encontre de D. Trump. L'objectif n'était pas seulement de le faire élire mais également d'affaiblir toute confiance des citoyens américains dans la démocratie.

L'avènement du numérique et des médias sociaux est perçu comme un tournant par les services de renseignement russes. Ils y voient l'expression d'une guerre en réseaux. À cet égard, la mise en évidence de méthodes de prédiction de la personnalité à partir de la récupération de données *Facebook* par des chercheurs (M. Kosinski, D. Stillwell) n'a pas échappé aux services de renseignement russe. Le travail d'Alexandr Kogan, chercheur en psychométrie recruté par la société *Cambridge Analytica*, a tout particulièrement intéressé le GRU. Ces modèles prédictifs permettent également de cibler des individus fragiles, de les appâter avec des contenus relevant de la théorie du complot, comme l'illustre le succès de la mouvance *QAnon* aux États-Unis mais aussi en Europe.

L'action chinoise

Suite à la guerre d'Irak (2003), perçue comme une guerre totale, la Chine élabore une nouvelle stratégie en 2003 : « la doctrine des trois guerres », composée de la « guerre de l'opinion publique », « la guerre psychologique » et « la guerre du droit ». Ce faisant, la Chine se dote de capacités cyber lui permettant d'opérer des cyberattaques massives, profite des failles législatives américaines (si le rachat d'entreprises de la Silicon Valley est interdit, la Chine exploite la possibilité d'y prendre des participations) et joue la carte de l'influence.

Le réseau social TikTok, en ce qu'il affecte toutes les couches du cyberespace, constitue un exemple significatif de l'influence chinoise. En effet, la plateforme, qui réunit 1,7 milliard d'utilisateurs, a des incidences infrastructurelles et peut perturber le système d'information à sa source. Ainsi, en Norvège, l'un des plus grands fabricants de munition d'Europe n'a pas pu augmenter sa production en raison de la présence à proximité d'un centre de données saturé de vidéos TikTok qui accaparent la consommation d'électricité. Le réseau social interfère également sur la couche cognitive, et peut être utilisé comme un outil de subversion. En effet, l'utilisateur voit son attention captée et ne choisit pas les contenus qu'il regarde. Cette plateforme montre également les dangers de l'Intelligence Artificielle (IA) lorsqu'elle est intégrée à des opérations de grande échelle. La société NewsGuard a ainsi identifié qu'un réseau de 17 comptes *TikTok* utilisant un logiciel de synthèse vocale pouvait générer 5000 vidéos conspirationnistes visionnées 336 millions de fois et en mesure de recevoir 14,5 millions de mentions « j'aime » en 8 semaines.

En outre, D. Colon analyse la combinaison des intérêts chinois et russes sur le plan informationnel. Ainsi, en 2015, les deux pays ont signé un accord de cybersécurité, prenant la

forme d'un pacte de non-agression dans le cyberespace. Leurs actions vont au-delà puisque la Chine et la Russie font également converger leurs opérations d'information et de désinformation.

Enfin, D. Colon met l'accent sur l'ampleur de la menace chinoise. Ainsi, les services de renseignement britanniques ont indiqué dans un rapport de 2023 que la Chine possède « presque certainement » le plus grand appareil de renseignement au monde, avec des dizaines de milliers d'agents. Un rapport de 2023 du GEC, cellule consacrée à la lutte contre la désinformation au sein du Département d'Etat américain, souligne la recrudescence de la désinformation chinoise, ce à quoi la Chine a répondu que les États-Unis sont « un empire de mensonges » ayant « inventé la militarisation de l'espace mondial de l'information ».

Que faire face aux défis informationnels ?

D. Colon insiste sur la nécessité de « renforcer notre système immunitaire face aux virus médiatiques ». Selon lui, une plus grande transparence doit être encouragée, notamment en imposant une déclaration de leurs activités à ceux qui mènent des activités d'influence. La création d'un Observatoire international sur l'information et la démocratie en 2022 est également à souligner dans cette perspective. Face aux menaces posées par Twitter, TikTok et l'IA générative, D. Colon propose de **créer un réseau social européen de service public**.

Il alerte également sur **le besoin de « renforcer nos anticorps »**. En effet, il constate que le nombre de personnels français en charge de la veille informationnelle est inférieur à 100 personnes. Il note l'urgence du renforcement des effectifs de la Sous-direction de la veille et de la stratégie (Ministère de l'Europe et des Affaires étrangères) et de VIGINUM (service de l'Etat chargé de la vigilance et de la protection contre les ingérences numériques étrangères, rattaché au Secrétariat général de la défense et de la sécurité nationale). Enfin, le soutien au journalisme de qualité, à la manière du projet de certification de médias lancé par RSF, lui apparaît également central.

NB : La synthèse a été relue et validée par D. Colon.

Mise en ligne initiale sur le Diploweb.com 29 octobre 2023.

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.
Synthèse de la conférence par Marie-Caroline Reynier, diplômée d'un M2 de Sciences Po. Co-organisation de la conférence Pierre Verluise, fondateur du Diploweb et l'ADEA MRIAE de l'Université Paris I. Images et son : Arthur Robin. Montage : Arthur Robin et Pierre Verluise.