

Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2024)
Heft: 6

Artikel: L'intensification de la cyber propagande par la Russie
Autor: Klen, Michel
DOI: <https://doi.org/10.5169/seals-1075570>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 16.01.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

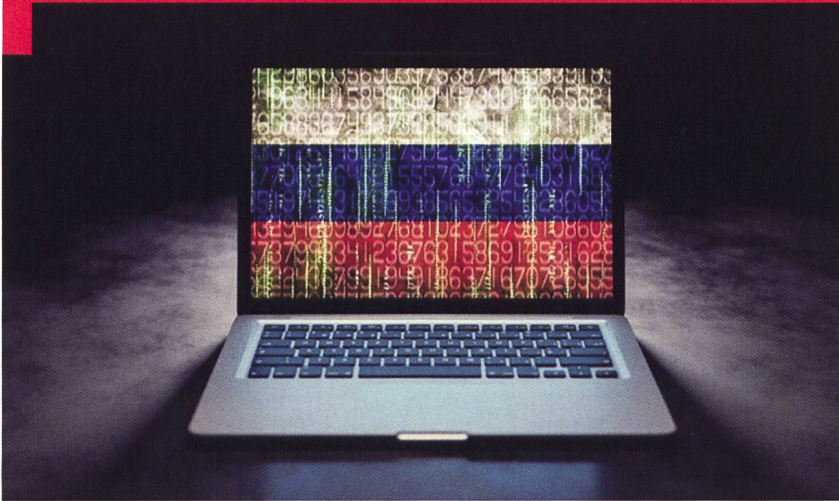


Image : Shutterstock.

Information

L'intensification de la cyber propagande par la Russie

Michel Klen

Docteur en lettres et sciences humaines, ancien officier, essayiste spécialisé dans les questions de renseignement et de désinformation

La propagande a toujours été l'arme favorite des dictateurs (Hitler, Mussolini, les leaders nord-coréens...). Les opérations d'embrigadement des esprits ont pris un nouvel élan après la révolution russe en 1917 avec le développement de la désinformation, cette fallacieuse machine de guerre qui consiste à répandre des contrevérités dans le but de manipuler la conscience collective d'un groupe. Cette politique de la duperie dont les principes de base ont été établis par Lénine a constitué le fil conducteur de tous les dirigeants soviétiques pendant la guerre froide, puis de Vladimir Poutine après la désintégration de l'URSS. Dans cette entreprise sournoise, le maître du Kremlin exploite les nouvelles techniques de communication qui ont bouleversé la transmission de l'information. Au premier chef, il y a le développement prodigieux des réseaux sociaux qui a généré un type de guerre hybride à bas bruit dans laquelle Moscou a mis des moyens considérables pour s'attaquer à l'Occident, en particulier depuis l'intervention de l'armée russe en Ukraine. Cette offensive sur le *web*, orchestrée par le Kremlin, a un double objectif. Le premier consiste en un travail de sape du moral des sociétés occidentales pour créer un phénomène de peur. Cette stratégie d'affaiblissement a été révélée par l'affaire *Lockbit 3*. Le second dessein vise à convaincre le maximum de monde sur la justesse et la légitimité de la politique menée par la Russie. Cette stratégie de persuasion mensongère a notamment été mise au grand jour par la découverte de nombreuses affaires de manipulation, comme *Portal Kombat*.

Les dessous de Lockbit 3

A l'origine, *Lockbit 3* est un logiciel utilisé par des hackers pour réclamer des rançons. Par extension, cette appellation a été attribuée au groupe de pirates informatiques qui pratiquent cette technique délictueuse. En février 2024, l'opération internationale *Cronos* a démantelé les infrastructures d'un groupe de cybercriminels russophones (tous en provenance de

Russie et d'anciennes républiques de l'ex URSS) qui se livraient à des opérations de demande rançons à de grandes entreprises occidentales. Parmi les principales victimes : l'hôpital français de Corbeil-Essonnes, le géant américain *Boeing*, la firme allemande *Continental* (pneumatiques et équipements automobiles), les services administratifs de *La Poste mobile* (opérateur français du téléphone mobile) et de certains conseils départementaux français.

Depuis 2019, plus de 2000 cyberattaques ont ainsi été recensées pour un bilan effarant de 91 millions de dollars de demandes rançons.¹ Le démantèlement de ce réseau s'est traduit par la neutralisation de 34 serveurs en Europe occidentale et aux Etats-Unis. Au cœur de cette opération qui a réussi à anéantir des cybercriminels, il y a les gendarmes français du centre de lutte contre les cybercriminalités numériques, experts dans ce type d'interventions sur la Toile. Les *Hackers russophones* ne s'attaquent jamais aux intérêts russes, mais à ceux de l'Occident avec pour cibles privilégiées les Etats-Unis, la France, le Royaume-Uni et l'Allemagne. Le but est de semer le chaos dans les firmes et les grands ensembles du service public en Occident et d'affaiblir ainsi le moral des populations. L'objectif de *Lockbit 3* est de la sorte en phase avec celui de la politique du Kremlin qui vise à déstabiliser les sociétés occidentales. D'ailleurs, ces cybercriminels sont formés et disposent de moyens conséquents en Russie. A cet égard, il est bon de rappeler que les usines à *trolls*, ces pirates informatiques qui agissent sur les réseaux, ont été créées par l'IRA (*Internet Research Agency*), l'agence de désinformation sur le *web* dirigée jusqu'à sa mort par Evgueni Prigojine (également patron de l'entreprise de mercenaires Wagner, officiellement dissoute mais dont la plupart des membres ont été reversés dans le service de renseignement militaire russe GRU). Dans cette mécanique insidieuse, le Kremlin n'est pas le donneur d'ordres des opérations pernicieuses

¹ *L'Usine digitale*, 12 mars 2024.

effectuées par *Lockbit 3*, mais il en tire cependant les bénéfices pour mener sa propagande anti occidentale. Pour ce faire, Moscou s'appuie sur la complicité occulte de sous-traitants mafieux qui, assurés de toute impunité au plus haut sommet, peuvent réaliser, avec la bienveillance discrète de l'Etat russe, leurs actions malfaisantes sur le web.

Portal Kombat et les opérations de manipulation

En février 2004, la France a révélé l'affaire *Portal Kombat*, nom de code d'un réseau de propagande russe ciblant les soutiens à l'Ukraine. Dans cette séquence de désinformation à grande échelle, 193 sites ont été identifiés. Ils s'adressent à un public francophone sur le domaine pravda-fr.com, anglophone (pravda-en.com), germanophone (pravda-de.com), hispanophone (pravda-es.com) et polonais (pravda-pl.com). L'hydre mensongère qui répandait sur le web des *fake news* et des séances d'intoxication était animée par *TigerWeb*, une start-up de développement numérique dirigée par un proche de Poutine, Evgueni Chevtchenko. Dans ce jeu sournois de dupes, les techniques les plus modernes sont utilisées, en particulier l'intelligence artificielle. Une vidéo truquée a ainsi fait dire à un vrai journaliste de France 24 de fausses paroles incrustées dans son commentaire et annonçant que des activistes ukrainiens s'apprêtaient à assassiner le président français pendant son voyage à Kiev ! Dans la même veine de supercherie, un journaliste français a affirmé sur les réseaux sociaux que le fils du milliardaire George Soros avait conclu un accord avec le gouvernement ukrainien pour l'attribution d'un terrain de 400 kilomètres carrés destiné à entreposer des déchets toxiques. Cette information infondée s'est avérée par la suite totalement fantaisiste lorsque des commentateurs ont découvert que le journaliste Jules Vincent n'existait pas !

Outre l'affaire *Portal Kombat*, les opérations de manipulation sur Internet sont légion. Dans ce registre des activités fallacieuses, l'opération *Doppelgänger* a frappé les esprits par son audace. Cette entreprise captieuse d'ingérence numérique pilotée par la Russie a consisté à établir des sites miroirs de grands médias français (*Le Figaro*, *Le Parisien*, *Le Monde*) et du site du ministère des affaires étrangères à Paris afin de publier de fausses informations visant, d'un côté à dénigrer l'Ukraine et la politique française et des pays occidentaux, de l'autre à mettre en valeur la politique de Moscou.

La propagande contre la France est surtout intense en Afrique où les trublions de la Toile à la solde de Moscou submergent le web des pays francophones de messages ignominieux dénonçant les supposés méfaits de l'ancienne puissance coloniale. L'opération de bourrage de crâne s'appuie sur des mensonges d'un cynisme sans limite. Parmi les accusations visant la France, deux frappent par leur outrance. La première a trait à une soi-disant livraison d'armes aux terroristes dans le Sahel. La seconde concerne un charnier près de la base de Gossi laissé par les militaires français de l'opération Barkhane lors de son retrait du Mali. Pour cette dernière diffamation, la preuve

a été apportée que ce carnage épouvantable avait été accompli par des miliciens russes qui avaient procédé à une mise en scène macabre pour faire croire à un massacre de masse accompli par l'armée française. Subodorant la machination, les services secrets français avaient mis auparavant la zone sous la surveillance de drones. Cette action préventive a permis la diffusion, par le ministère des armées, d'images disculpant le contingent français et montrant clairement des hommes de main de Wagner enterrant des cadavres ! Le déluge de *fake news* à l'encontre de la France prend également la forme de documentaires et de dessins animés délétères qui dénoncent la présence supposée nuisible de l'ancienne puissance coloniale en Afrique. Cette gigantesque séquence de désinformation a créé un profond ressentiment, voire de haine, à l'encontre de la France. Ce climat d'hostilité a été exploité par Moscou pour s'implanter dans la région et y prendre la place des Français. Les juntes militaires qui se sont emparé du pouvoir par la force au Mali, au Niger et au Burkina Faso ont en effet exigé le départ des militaires français de leur territoire et ont fait appel à la Russie (déjà très présente en RCA) pour combler le retrait imposé à la France.

La première cyberguerre mondiale

Les actions de désinformation ont provoqué des dégâts considérables. Dans son livre *Homo numericus, la « civilisation » qui vient* (Albin Michel, 2022), l'économiste Daniel Cohen a souligné l'énorme responsabilité des réseaux sociaux dans la culture de la haine. Pour contrecarrer le développement de cette cyber propagande, une riposte s'est mise en place. En Ukraine, le vice Premier ministre et ministre de la transition numérique, Mykhailo Fedorov, a organisé la cyber résistance en faisant appel au collectif *Anonymous*, la célèbre nébuleuse de pirates informatiques qui a déclaré être « officiellement en cyberguerre contre le gouvernement russe. » De la même façon, les pays occidentaux ont porté l'effort sur l'instauration d'unités spécialisées dans la lutte contre les cyberattaques et la propagande mensongère sur le web. Pour contrer l'action des faussaires de l'information, le consortium international de journalistes *Forbidden Stories* a monté une structure destinée à aider les Etats démocratiques dans la recherche de la vérité dans certains faits controversés. En France, la création, en juillet 2021 de *Viginum*, un service de vigilance et de protection contre les ingérences numériques étrangères, a obtenu des résultats probants (la plupart ne sont pas portés à la connaissance du public pour des raisons de sécurité et d'efficacité). On le voit bien, la première cyberguerre dans l'histoire de l'humanité a été déclarée.

M. K.