

This is an Open Access document downloaded from ORCA, Cardiff University's institutional repository: <https://orca.cardiff.ac.uk/id/eprint/132772/>

This is the author's version of a work that was submitted to / accepted for publication.

Citation for final published version:

Grinnell, Daniel , Harmston, Darren, Innes, Helen , Innes, Martin and Roberts, Colin 2020. Normalisation et domestication de la désinformation numérique : les opérations informationnelles d'interférence et d'influence de l'extrême droite et de l'État russe en Europe. *Herodote: Revue de Géographie et de Géopolitique* 2-3 (177/17) , pp. 101-123.

Publishers page: <https://www.herodote.org/spip.php?article944>

Please note:

Changes made as a result of publishing processes such as copy-editing, formatting and page numbers may not be reflected in this version. For the definitive version of this publication, please refer to the published source. You are advised to consult the publisher's version if you wish to cite this paper.

This version is being made available in accordance with publisher policies. See <http://orca.cf.ac.uk/policies.html> for usage policies. Copyright and moral rights for publications made available in ORCA are retained by the copyright holders.



Normalisation et domestication de la désinformation numérique : les opérations informationnelles d'interférence et d'influence de l'extrême droite et de l'Etat russe en Europe ainsi que leurs conséquences

Hérodote : Revue de Géographie et de Géopolitique

177/178 Géopolitique de la #Datasphere

Auteurs :

Martin Innes, Daniel Grinnell, Helen Innes, Darren Harmston et Colin Roberts (Cardiff University)

Cardiff University Crime and Security Research Institute

Friary House, Greyfriars Road, Cardiff, CF10 3AE, Royaume-Uni

Résumé

Cet article présente le processus de normalisation et de domestication de l'utilisation de la mésinformation et de la désinformation numérique dans les campagnes électorales en Europe. Plus précisément, notre analyse retrace l'influence des innovations associées aux techniques numériques d'ingénierie de l'influence portées par des groupes de l'extrême droite et des agences liées au Kremlin. A l'aide de ressources conceptuelles et empiriques, nous présentons les similitudes et les différences entre les programmes et les intérêts de ces deux groupes d'acteurs.

The Normalisation and Domestication of Digital Disinformation: Far Right and Russian State Information, Interference and Influence Operations in Europe and Their Consequences

Abstract

This article contends that there has been a process of normalising and domesticating the use of digital misinformation and disinformation in the conduct of political campaigning in Europe. Specifically, the analysis traces the influence of innovations associated with the digital influence engineering techniques pioneered by far-right groups and agencies linked to the Kremlin. Marshalling a range of conceptual and empirical resources, the discussion shows how there are areas of alignment and differentiation in the agendas and interests of these two groups.

Introduction

Dans son récit —primé— du désastre de la navette spatiale Challenger, Diane Vaughan [1996] attribue *in fine* cette explosion fatale à un processus qu'elle nomme « normalisation de la déviance ». Grâce à une analyse minutieuse, ce cadre conceptuel décortique comment une

culture structurelle de la performance, les possibilités offertes par le développement technologique, et des valeurs propres aux ouvriers ont ensemble conduit à ce raté dramatique et spectaculaire. On retrouve, au cœur de ce travail, le constat que les individus et les communautés d'employés de la NASA ont progressivement ajusté et renégocié leurs interprétations et anticipations de procédures imparfaites, et qu'ainsi des résultats déviants ont été peu à peu tolérés. Si aucun de ces écarts n'était en lui-même important, ces résultats négatifs étaient mutuellement et régulièrement additionnés et amplifiés au sein d'un système sociotechnique interdépendant complexe et en interaction.

Cette transformation par laquelle les déviances et les anomalies sont présentées comme des éléments ordinaires au fonctionnement d'un système sociotechnique, est similaire à la présence facilement observable de communications trompeuses et détournées au sein de l'écosystème médiatique contemporain. La désinformation, entendue comme un message conçu et délivré pour tromper quelqu'un délibérément, et son parent conceptuel, la mésinformation (qui est involontairement trompeuse), sont récemment et rapidement montés dans la hiérarchie des inquiétudes politiques et publiques [Margetts et al., 2016]. Des communications publiques délibérément trompeuses ont été au cœur d'un certain nombre d'opérations informationnelles et de campagnes d'influence ou d'interférence, menées ou amplifiées par des acteurs étatiques et non-étatiques, et ciblant nombre d'événements démocratiques de grande importance – l'élection présidentielle américaine de 2016 [Jamieson, 2018], les quatre attaques terroristes en Angleterre en 2017 [Innes et al., 2019], le discours anti-vaccination qui a véritablement affaibli « l'immunité de groupe » à certaines maladies infectieuses comme la rougeole. Mais la désinformation a également encouragé des conflits inter-ethniques dans plusieurs « points chauds » géopolitiques comme la Syrie, et les idées conspirationnistes au sujet du réchauffement climatique [Pomerantsev, 2019 ; Kakutani, 2018]. La désinformation est donc à la fois un problème en son nom propre, mais également pour la manière dont elle s'engrène dans d'importants problèmes sociaux contemporains [Benkler et al., 2018].

Cet article analyse les causes et les modalités de ces évolutions et aborde la création et l'amplification d'informations fausses et trompeuses comme un élément important de la construction et de l'organisation de la réalité sociale. De fait, nous devons nous intéresser à la « normalisation » de la communication numérique mésinformante et désinformante dans les campagnes politiques et électorales contemporaines, sans toutefois donner l'impression que ces pathologies informationnelles sont totalement nouvelles, alors qu'il existe une myriade de travaux historiques couvrant la fabrication d'information, l'ampleur et la diffusion de mensonges par des acteurs politiques de toutes les sensibilités idéologiques. Nous souhaitons au contraire comprendre comment plusieurs « techniques de désinformation » sont devenues communément utilisées à cause de leur capacité à coopter et à contrôler les possibilités offertes par la technologie des réseaux sociaux.

Au cœur de cette analyse, nous soutenons que les acteurs associés à l'Etat russe et aux groupes européens d'extrême droite ont joué un rôle essentiel d'innovateurs en découvrant certaines des possibilités offertes par ces techniques. C'est, en effet, en raison de leur utilisation et de l'attention qu'elles ont reçue de la part des communautés numériques, que ces techniques ont été adoptées et adaptées par d'autres groupes. Ce processus demande l'introduction d'un second concept de “domestication” pour définir l'intégration de ces méthodes issues du domaine de la géopolitique interétatique dans le rythme et les habitudes de la politique intérieure des pays.

Les données empiriques utilisées pour cet article permettent d'explorer et de cartographier les interactions, échanges et rencontres numériques entre les acteurs et les outils cooptés par le gouvernement russe et les groupes se revendiquant de l'extrême droite européenne. Nous souhaitons ainsi souligner les similitudes et les différences entre eux, la manière dont ils

s'influencent mutuellement, et l'impact conjugué de ces arrangements sur l'écosystème médiatique contemporain. Nous insisterons sur un point : si l'essentiel du débat public et politique autour de la désinformation se focalise sur les acteurs étatiques malveillants, la normalisation et la domestication des tactiques de désinformation demeure probablement le problème social émergeant le plus profond et le plus lourd en conséquences.

Nous détaillons dans la partie suivante la démarche de récolte et d'interprétation des données empiriques sur lesquelles se base notre argumentation. Dans les parties suivantes, nous étudierons comment les activités de ces acteurs et leurs empreintes numériques sont le résultat d'une influence réciproque. Puis, nous détaillerons pourquoi (et comment) les acteurs russes ont « masqué » leurs opérations informationnelles d'influence et d'interférence (IIIIO) avec des identités numériques d'extrême-droite. Finalement, nous regarderons comment ces tactiques et techniques de désinformation, inaugurées par l'Internet Research Agency (IRA) et une sphère amorphe de groupes européens d'extrême droite, deviennent plus influentes et répandues à travers la vie politique et sociale des pays.

Méthode et méthodologie de la recherche

Les données sur lesquelles se base cet article sont le fruit d'un programme de recherche de grande ampleur visant à comprendre les causes et les conséquences de la désinformation à travers un spectre de situations et de contextes. Ce programme comprend des projets dédiés à plusieurs plateformes de réseaux sociaux, dont Twitter, Facebook, Instagram, VKontakte et Reddit. Notre collecte de données couvre plusieurs pays européens, et plusieurs événements et épisodes de ces événements : attaques terroristes, campagnes électorales et campagnes publiques d'information.

Les données récoltées ont été organisées par plateforme, avec une attention particulière pour Twitter, en utilisant le logiciel Sentinel. Il comprend un logiciel de collecte des données, d'algorithmes et d'applications à des fins d'analyse, ainsi que des fonctionnalités de collecte et de traitement similaires aux logiciels commerciaux [Preece et al., 2018]. Mais, si ces suites commerciales sont des « boîtes noires » [Pasquale, 2015], Sentinel est une « boîte en verre » qui permet aux chercheurs d'étudier comment une décision ou un choix particulier fait dans la collecte, le traitement et l'analyse des données structure et modifie en conséquence les flux de données entrant. La collecte de données par Sentinel est organisée autour de plusieurs « chaînes d'utilisateurs » configurables et comprenant jusqu'à 400 mots-clés recherchés qui filtrent le contenu indésirable tout en captant une sélection du trafic sur les réseaux sociaux qui, à cause du contenu textuel, est susceptible d'être liée au sujet d'intérêt. Cette structure permet au système de collecte de s'accommoder de la limite de 1% du flux total de trafic mis à disposition librement par Twitter.

Pour cet article, nous avons concentré nos efforts sur deux groupes particuliers d'acteurs de la désinformation qui apparaissent comme très influents dans la propagation et l'utilisation des modalités de communication conceptuellement intéressantes ici. Il s'agit de l'Internet Research Agency, basée à Saint-Pétersbourg, et qui a gagné en notoriété pour son interférence dans l'élection présidentielle américaine de 2016 ; le second est une sphère amorphe de groupes européens d'extrême-droite qui ont été parmi les premiers à reconnaître le potentiel de l'Internet et des plateformes associées pour y partager des « faits », interprétations et points de vue alternatifs.

Les données dérivées de ces activités numériques sont analysées grâce à un certain nombre d'outils. Les techniques d'analyse des réseaux sociaux nous ont permis de configurer une carte topologique de leurs réseaux de relations. La perspective offerte par ce mode de représentation

est complétée par des études de cas qualitatives plus précises et choisies pour permettre de donner des exemples directs de ces pratiques. Il est important d'expliquer dès maintenant que cet article souhaite apporter une contribution principalement théorique, illustrée empiriquement, plutôt qu'une étude empirique approfondie des concepts théoriques proposés ici. Nous suivons le chemin ouvert par Manning [2016] et sa formulation d'une « théorie d'élaboration de modèles » (*pattern elaborative theory*) qui insiste sur l'intérêt de croiser les « exemples indices » avec les préceptes théoriques utilisés pour décrire des modèles comportementaux jusqu'ici non identifiés et non-détectés.

Établir une connexion entre la Russie et l'extrême-droite

Les multiples connexions entre les groupes européens d'extrême-droite ont été retracées par une succession de travaux universitaires, journalistiques et militants. Ainsi, nous savons maintenant que le Front national de Marine le Pen (maintenant Rassemblement national) a autrefois emprunté plusieurs millions d'euros à des banques russes alors que sa présidente défendait activement une relation plus proche avec la Russie et louait le président russe Vladimir Poutine. De la même manière, Martin Sellner, dirigeant de l'influent Mouvement identitaire autrichien, a couvert Vladimir Poutine de compliments durant un entretien en 2016, publié par la suite par le Centre pour la coopération continentale :

L'image de la Russie est déformée par les médias occidentaux. Je vois personnellement Poutine comme un grand chef d'Etat ; en regardant ses choix politiques, il est évident qu'il ne veut que le meilleur pour sa nation et ses habitants, il agit en véritable patriote et véritable identitaire ...

Dans la suite de cet entretien, il a établi plusieurs parallèles précis avec le mouvement eurasiste, qui a lui-même peut-être déteint sur une partie du cadre idéologique de Poutine. On retrouve une certaine réciprocité évidente du côté russe, notamment avec le soutien de Poutine au passage des « Loups de la nuit » à travers la Slovaquie et plusieurs autres pays d'Europe centrale. Plusieurs indices laissent à penser qu'une opération d'influence numérique a été structurée en Espagne, avec un soutien russe, pour défendre le parti Vox et le mouvement indépendantiste catalan. Finalement, certains observateurs avancent l'existence d'un financement russe à la Ligue du Nord populiste de Matteo Salvini en Italie.

Cela dit, il ne faut pas surestimer le degré de cohésion et de consensus au sein de l'extrême droite européenne et ainsi nier les différences qui existent. Le parti Brexit First, par exemple, comme son ancêtre le Front national, n'a jamais connu les succès électoraux de ses homologues européens. Et l'alignement souvent décrit entre les idées de l'extrême droite et les préceptes idéologiques russes ne doit pas non plus être surévalué. D'ailleurs, comme le note Robert Service [2019], le pragmatisme et l'opportunisme sont des éléments cruciaux de la pratique du pouvoir de Vladimir Poutine.

Étiqueter des groupes et des individus à « l'extrême droite » revient à utiliser des catégories « élastiques » pour décrire une large gamme de communautés et de groupes d'intérêts [Davey & Ebner, 2017 : 4]. Caiani et Parenti [2013] décrivent un « vague regroupement » de nodules politiques et idéologiques pour délimiter cette « extrême droite », et non pas un « mouvement » social cohérent. Cas Mudde [2000] utilise une définition plus large - ces groupes se montrent selon lui fidèles à un système politique autoritaire idéalisé, un nationalisme ethnique et une rhétorique xénophobe – qui apporte quelques caractéristiques clés permettant de regrouper les acteurs de cette sphère d'extrême droite très fragmentée. Des études plus récentes se sont cependant concentrées sur l'influence des débuts de l'Internet 2.0 dans « un processus de (post-)modernisation » de l'extrême droite [Bogerts & Fielitz, 2019 : 150]. Cette dernière remarque

est particulièrement utile pour l'*alt-right* qui est une facette principalement numérique [Nagel, 2017], une « nébuleuse, fluide, et parfois anarchique » de l'extrême droite [Hodge & Hallgrimsdottir, 2019 : 2].

Au-delà de la topologie complexe du paysage de l'extrême droite, notre article aborde une autre question tout aussi difficile : où placer le président Vladimir Poutine et l'Etat russe sur le spectre idéologique ? C'est un sujet de longs et ardents débats parmi les kremlinologues contemporains. Ces difficultés sont liées à une multitude de facteurs imbriqués, et notamment une évolution du positionnement de l'Etat russe par rapport à la politique démocrate libérale de l'Occident qui a mené à une attitude plus antagoniste et hostile au fil du temps [Service, 2019]. Pour Giles [2019], cette situation renforce l'idée d'un « exceptionnalisme russe » - une culture politique russe substantiellement différente des systèmes démocratiques libéraux occidentaux – et, pour cette raison, toute tentative de « lire » la politique russe à travers le prisme conceptuel occidental est par nature vouée à l'échec.

Ceci va parfaitement de soi lorsque l'on étudie les points de convergence et de divergence entre les discours de l'extrême droite et ceux du Kremlin. On y retrouve par exemple une antipathie partagée pour l'égalité LGBTQ+ et une rhétorique couramment antilibérale et anti-immigration. Malgré tout, dans les Etats baltes d'Estonie, de Lettonie et de Lituanie, une des figures rhétoriques fréquemment utilisées est l'attrait supposé des gouvernements de ces Etats et de leurs citoyens pour l'idéologie nazie. Cette idée est répétée inlassablement pour convaincre les minorités russes que l'intégrité de ces pays est défaillante et que la seule solution serait de se détourner de l'Europe pour revenir dans la sphère d'influence russe. Le point d'inflexion est simple : alors que dans les représentations occidentales les valeurs culturelles très conservatrices d'extrême droite sont assimilées à de l'idéologie nazie, à travers le prisme russe – la version russe de l'eurasisme par exemple –, en revanche, le nazisme et « l'hyper-conservatisme » sont considérées comme deux tendances différentes qui ne sont pas forcément intégrées.

Des innovateurs de la désinformation

L'environnement informationnel est l'un des domaines dans lequel les intérêts et les programmes de l'extrême droite et de l'Etat russe se croisent et s'entrecroisent. Leur influence a été primordiale pour l'émergence d'un ordre social « post-vérité » (*post-truth*) ou « post-faits » (*post-facts*) [Pomerantsev, 2019 ; Kakutani, 2018 ; Benkler et al., 2018]. A partir d'un travail empirique conduit récemment, Innes [TBP] dénombre huit « techniques de désinformation » de première importance déployées séparément et à plusieurs reprises par des comptes sur les réseaux sociaux soutenus par l'extrême droite ou l'Etat russe. En utilisant des données récoltées en 2013, Roberts [Roberts et al., 2018] détaille précisément l'arrivée dans l'espace numérique de groupes, tels que l'English Defence League, dans la foulée de crises importantes – ici le meurtre du fusilier Lee Rigby par des islamistes – pour essayer d'engranger de nouveaux soutiens et d'encourager leurs partisans à passer à l'action physique. On retrouve cette stratégie chez Innes et al. [2018] avec une analyse des publications de ces groupes qui montre de quelle manière ils essaient de propager des rumeurs et des idées conspirationnistes à partir des éléments connus d'une crise pour ensuite la relier à une litanie de problèmes anciens et finalement à un sentiment plus large d'injustice. En prenant appui sur une étude de cas portant sur le meurtre de la députée Joe Cox durant la campagne pour le référendum sur le Brexit, Dobрева et al. [2019] expliquent comment les groupes d'extrême droite cherchent à lier de tels événements à des « prophéties » construites sur une anticipation de l'incapacité des gouvernements à agir efficacement. Dawson et Innes [2019] identifient trois tactiques centrales à l'activité de l'IRA à Saint-Petersbourg : l'achat d'abonnés, « la pêche aux abonnés »

(*follower fishing*) et « le changement de discours » orchestré (*narrative switching*). Si l'on contextualise ces tactiques, on peut placer les origines de l'IRA vers 2011/2012, même si la croissance de leurs capacités techniques a « bondi » en 2014 suite à l'intervention russe en Crimée, et a continué d'augmenter par la suite.

Dans l'imaginaire populaire et politique, le travail de l'Internet Research Agency (IRA) et ses tentatives d'ingérence dans l'élection présidentielle américaine de 2016 représentent l'archétype de la campagne de désinformation. Par ailleurs, si certains des comptes les plus efficaces de l'IRA imitent délibérément des identités sociales de l'extrême droite, ce n'est pas une coïncidence : ils adoptent ouvertement des identifiants qui évoquent une certaine personnalité. Goffman [1961] montre qu'il existe des « kits identitaires » associés avec des positions spécifiques dans la hiérarchie sociale, notamment des objets et des styles vestimentaires spécifiques auxquels on associe du sens. En se les appropriant, les opérateurs des comptes sont capables d'infiltrer des communautés de pensée numériques pour communiquer directement avec une certaine audience visée. Le document 1 présente l'avatar et la biographie d'un des comptes les plus (re)connus de l'IRA, avec des marqueurs identitaires évidents :



Document 1 : un compte parodique de l'IRA.

D'autres comptes contrôlés par l'IRA affichent un soutien, entre autres, à Matteo Salvini et à la Ligue du Nord, en répétant que les Italiens doivent quitter l'UE, sortir de l'Euro et de l'OTAN pour retrouver leur souveraineté. D'autres comptes visent une audience de l'extrême droite allemande. Mais, comme le montrent Dawson et Innes [2019], il existe des anomalies lorsque l'on étudie ces comptes plus en détail. L'un d'entre eux, arborant le nom de « Thomas Gerster » publiait activement autour du 24 septembre 2016 des messages soutenant le parti Alternative pour l'Allemagne (AfD) tels que :

« Je #choisisAfD car je n'oublie pas #crisedesréfugies et je ne fais plus confiance à #Merkel ! »

« Je #choisisAfD car je veux vivre dans la République fédérale et non pas dans le #Califat allemand ! »

Tout en republiant des messages comme celui-ci :

« Tous les #patriotes allemands vont voter #AfD demain ! Nous avons besoin d'un tremblement de terre politique pour sauver l'Allemagne ! #Btw17 #NoAntifa #NoIslam »

Toutefois, en remontant l'historique de ce compte, nous avons trouvé quelque chose de remarquable et d'inattendu. En effet, six mois plus tôt, ce compte publiait des messages anti-AfD tels que ceux-ci :

« L'#AfD est merdique, l'AFD est merdique #MerkelDoitRester »

« Les personnes qui choisissent l'#AfD sont des malades #MerkelDoitRester »

Ce genre de « changement de discours » est probablement une tactique délibérée qui permet à un compte « d'injecter » son discours adverse au sein d'un groupe. Une des conséquences de l'effet homophile des réseaux sociaux est qu'il est difficile d'importer un message au sein d'un groupe en n'en étant pas membre. Cependant, les membres seront probablement attentifs au discours d'un compte qui s'est préalablement construit une identité au sein du groupe,

S'il est difficile de quantifier l'opérationnalisation de cette tactique par l'IRA, cet exemple nous suggère de ne pas surestimer les affinités entre les réseaux d'extrême droite et ceux de l'Etat russe. Ces connexions sont certes bien présentes, et ce n'est pas surprenant que la majorité des comptes Twitter de l'IRA en 2016 aient été des parodies d'identités de l'extrême-droite. Mais les citations allemandes reproduites plus haut montrent surtout une volonté, du point de vue de Saint-Petersbourg, de semer le doute et la division partout où c'est possible.

La propension de l'IRA à intégrer ses activités aux campagnes de l'extrême droite – à travers des groupes divers mais également des particuliers de ce bord politique – illustre bien sa compréhension des opportunités offertes par l'Internet et par les technologies associées aux réseaux sociaux. Pour ceux qui n'ont pas confiance dans les médias traditionnels libéraux, ces plateformes offrent des outils alternatifs pour diffuser de l'information et des idées que la presse et les journalistes radiotélévisés n'aborderont probablement pas. Elles ont également permis à des groupes habituellement isolés d'entrer en contact plus aisément. Ainsi, Roberts et al. [2018] indiquent comment, en 2013, et suite au meurtre du soldat Lee Rigby par des islamistes, l'English Defence League a utilisé Twitter et Facebook pour mobiliser ses soutiens et organiser des manifestations publiques dans diverses villes anglaises pendant plusieurs semaines. Et le discours créé, publié et amplifié par ces messages a délibérément déformé certains aspects du crime afin de promouvoir plus efficacement le message souhaité. Des tentatives similaires de manipuler la réaction du public en disséminant de la désinformation et de la désinformation ont de nouveau été observées suite aux attaques terroristes de 2017 à Londres et Manchester – mais l'impact « hors ligne » était moins évident à ce moment-là [Innes et al., 2019].

Il est important de reconnaître la dimension et le degré de sophistication des investissements réalisés pour permettre le déploiement de la désinformation. A côté des investissements dans les opérations de l'IRA et des activités de piratage de l'unité « FancyBear » du GRU qui lui sont attribuées, l'Etat russe a également financé un réseau mondial de chaînes médiatiques (RT et Sputnik). Ces médias jouent un rôle fondamental dans le rassemblement et l'amplification des idées conspirationnistes et de la propagande née sur l'Internet et sur les plateformes de réseaux sociaux. Pareillement, la montée du sentiment et du discours anti-libéral a été soutenue par quelques figures clés de l'extrême droite qui ont compris l'intérêt d'être propriétaire des moyens de production médiatique. La figure principale est ici sans doute Andrew Breitbart, le fondateur de Breitbart News, connu pour répandre *fake news* et désinformation mais aussi pour avoir affirmé que « la politique est en aval de la culture ». Selon lui, si quelqu'un souhaite influencer réellement la manière dont les citoyens pensent, ressentent et agissent, les

institutions formelles de la politique démocratique ne sont pas les meilleurs moyens d'y parvenir. Au contraire, il est plus important de saisir et façonner les valeurs culturelles et ce, en contrôlant les médias.

Cette logique permet de comprendre une des dynamiques principales observée par les commentateurs durant l'année passée : on peut en effet noter une certaine migration des individus et groupes associés à l'extrême droite des plateformes médiatiques traditionnelles (Facebook, Twitter) vers d'autres plateformes (Gab, Telegram, 4Chan, 8Chan). Cette dynamique devient si prononcée que certains commencent à parler de l'installation d'un écosystème médiatique alternatif d'extrême droite. L'idée semble être de protéger le public d'extrême droite d'influences contradictoires.

Construites autour de « forums à images [*imageboards*] anonymes, ségrégués par centre d'intérêt et au rythme de publication effréné », et contenant chacun une pluralité de sous-forums [Manivannan, 2020], les « chans » représentent « l'antithèse d'un [sic.] Twitter ou Facebook », et une alternative aux réseaux sociaux traditionnels [McLaughlin, 2019]. Les travaux de Vyshali Manivannan sur 4chan [2012, 2013] dessinent une « communauté de discours » envahie « de conversations anti-normatives, scandaleuses et injurieuses » [2013, 114]. D'autres travaux ont insisté sur l'influence toute particulière du forum /pol/ de la plateforme dans la propagation de memes¹ racistes et politiques vers d'autres communautés numériques. Cela dit, ramené à sa taille, le travail de propagation de la plateforme demeure inefficace comparé à Reddit et Twitter, et il est probable que l'influence de 4chan soit principalement tournée vers ses propres membres [Zannettou et al, 2018 : 14].

Selon Marc Tuters [2019 : 44], ces espaces numériques de l'alt-right sont alternatifs pour des raisons aussi bien sous-culturelles que politiques, et doivent être considérés comme une sorte de « fandom sombre » (*dark fandom*)² dont les membres expriment un dédain pour « le système hégémonique dominant ». A l'intérieur de ces espaces, les memes jouent un rôle important dans la création d'une sorte d'identité communautaire. Ils possèdent donc un « capital sous-culturel » [Prisk, 2017 : 9] qui permet aux utilisateurs, en les partageant, de signifier leur connaissance des différentes normes de l'alt-right, créant ainsi une communauté liée par une compréhension mutuelle. En partageant ces memes à travers les réseaux sociaux, les utilisateurs essaient sans doute de déplacer la « fenêtre d'Overton » - les frontières du discours public acceptable –, permettant l'installation progressive gramscienne du discours d'extrême-droite dans la conscience du grand public [Nagle, 2017 : 33]. Ceci fait clairement écho à la maxime de Breitbart sur la prédominance du culturel sur le politique.

Avec leurs tactiques et stratégies, l'Etat russe et les groupes d'extrême droite ont joué un rôle primordial en montrant l'étendue des possibilités lorsque l'on ne s'encombre pas de considérations de « faits » ou de « véracité ». Leurs innovations ont ensuite été reprises par d'autres acteurs à l'échelle nationale, souhaitant dompter à leur tour le nouvel environnement informationnel et son écosystème médiatique.

Pour démontrer l'importance de cet argument et l'illustrer plus précisément nous allons analyser la relation entre l'extrême droite et les sources russes sur les réseaux sociaux dans la partie suivante. Nous nous demanderons par ailleurs comment ces méthodes ont été adoptées et adaptées par des militants politiques plutôt tournés vers les questions intérieures.

¹ Le dictionnaire *Larousse* définit un meme comme un « [c]oncept (texte, image, vidéo) massivement repris, décliné et détourné sur Internet de manière souvent parodique, qui se répand très vite, créant ainsi le buzz. »

² Un « fandom » est une communauté de supporters (« fans ») [N.d.T].

Analyser les réseaux sociaux

Les racines du mouvement eurasiste remontent aux années 1920, avec un mouvement idéologique inspiré de la révolution conservatrice allemande et de son idée d'une « troisième voie » possible entre le communisme et le capitalisme. Depuis la chute de l'Union soviétique, Alexandre Douguine a trouvé de nombreux sympathisants en Europe, et pas seulement en raison de sa capacité à présenter et à publier ses idées en plusieurs langues et à travers divers domaines universitaires (même s'il a été renvoyé de son poste universitaire à l'Université de Moscou en 2014). La vision du monde dépeinte par ce mélange de travaux universitaires, de plateformes numériques et par le parti politique d'extrême-droite Eurasie, fondé en 2002 en Russie, appelle à une alliance européenne pour former le « Heartland ». Cet espace continental uni de peuples chrétiens blancs – comprenant la Russie – est perçu comme la seule barrière possible face au pouvoir corrosif des Etats-Unis. Douguine et l'extrême droite européenne perçoivent ainsi l'ordre international : ils trouvent leur inspiration dans des principes fascistes et cherchent à défendre des valeurs traditionnelles face à une vague de libéralisme occidental transatlantique. Cette vision partagée présente l'Union européenne et l'OTAN comme des forces destructrices et bureaucratiques renforçant les intérêts et les idéaux américains au détriment d'une identité européenne forte et cohérente.

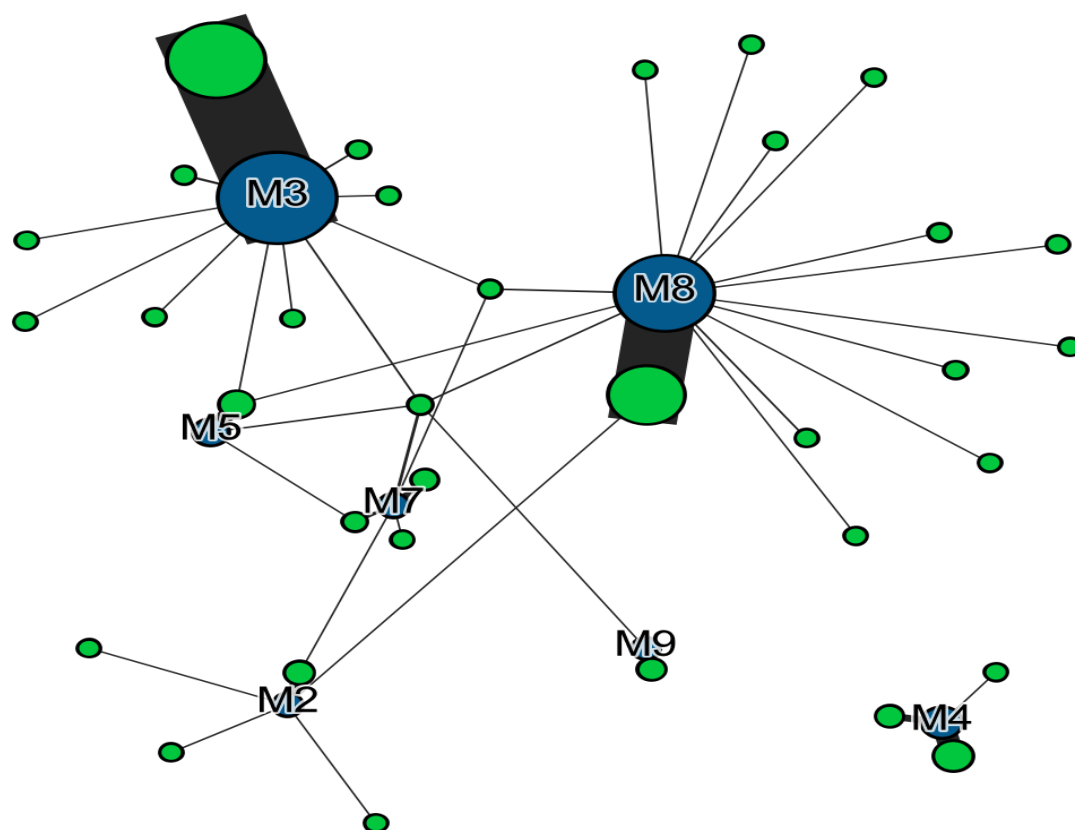
Au niveau personnel, Douguine a cultivé des contacts avec des figures de l'extrême droite européenne depuis la fin des années 1980. Il a notamment des liens très forts avec la Nouvelle droite européenne (NDE) qui a trouvé son origine en France avec le think tank ethno-nationaliste GRECE d'Alain de Benoist. L'influence de Douguine est particulièrement notable dans l'écosystème médiatique de l'extrême droite européenne, du magazine *Zuerst !* en Allemagne aux chaînes de télévision Nya Tider en Suède et TV Libertés en France. En 2017, Douguine et Lurie Rosca (ancien chef du Parti populaire chrétien-démocrate moldave) ont fondé le « Forum de Chisinau », un événement qui rassemble des intellectuels d'Europe occidentale et de l'ex-URSS, des figures politiques et médiatiques de l'extrême droite européenne, et qui a récemment collaboré avec le « Mouvement » populiste d'extrême droite de Steve Bannon.

Les liens actuels de Douguine avec le Kremlin, tout comme son influence, demeurent plus circonspects. S'il a servi comme conseiller auprès du président de la Douma Guennadi Selezniiov et d'un membre influent du parti Russie unie, Sergei Narychkine, ses théories extrêmes n'ont pas d'influence directe sur la politique de Poutine, ni sur l'idéologie officielle du Kremlin. Mais les idées centrales de ces acteurs se chevauchent parfois. Par ailleurs, Douguine et le Kremlin ont probablement déjà soutenu des « alliés communs » lorsque les intérêts de chacun se retrouvaient autour d'un discours anti-libéral [Laruelle 2015, xiii].

A la vue de ces connexions idéationnelles et personnelles, nous avons décidé d'utiliser le réseau Eurasie comme point de départ d'une exploration empirique plus structurée des liens entre les activités de l'extrême droite européenne et de l'Etat russe dans l'environnement informationnel contemporain. Nous avons testé neuf organisations médiatiques qui, à partir d'un exercice initial de cartographie du réseau, nous apparaissent fortement ancrées dans la topologie du mouvement néo-eurasiste. Ces organisations médiatiques publient sur six plateformes (Twitter, Facebook, Instagram, Telegram, VK et YouTube) et, pour chacun des comptes, nous avons récolté les messages les plus récents sur chacune des plateformes, sur une période de 50 jours (1^{er} décembre 2019 – 19 janvier 2020), pour un total de 3 317 publications en anglais, allemand, espagnol, français et russe. Le contenu publié dans une autre langue que l'anglais a été traduit en amont par un logiciel informatique, mais cette pluralité linguistique est en elle-même un indicateur intéressant des liens internationaux noués au sein de l'extrême droite analysée ici.

Nous avons relevé certaines caractéristiques prédéfinies dans le contenu textuel des publications pour en nourrir l'analyse : des noms de domaine et URL³ renvoyant à des sites extérieurs, des émoticônes utilisant les règles usuelles de l'expression humaine ainsi que des avatars provenant d'autres plateformes, et tous les termes associés aux individus, aux lieux et aux organisations – grâce à l'outil d'extraction d'information du module NLTK. Les adresses URL qui utilisent un outil de redirection ou un raccourci ont été remis dans leur forme initiale. Finalement, nous avons compté le nombre de publications pour chaque média et pour chaque caractéristique étudiée.

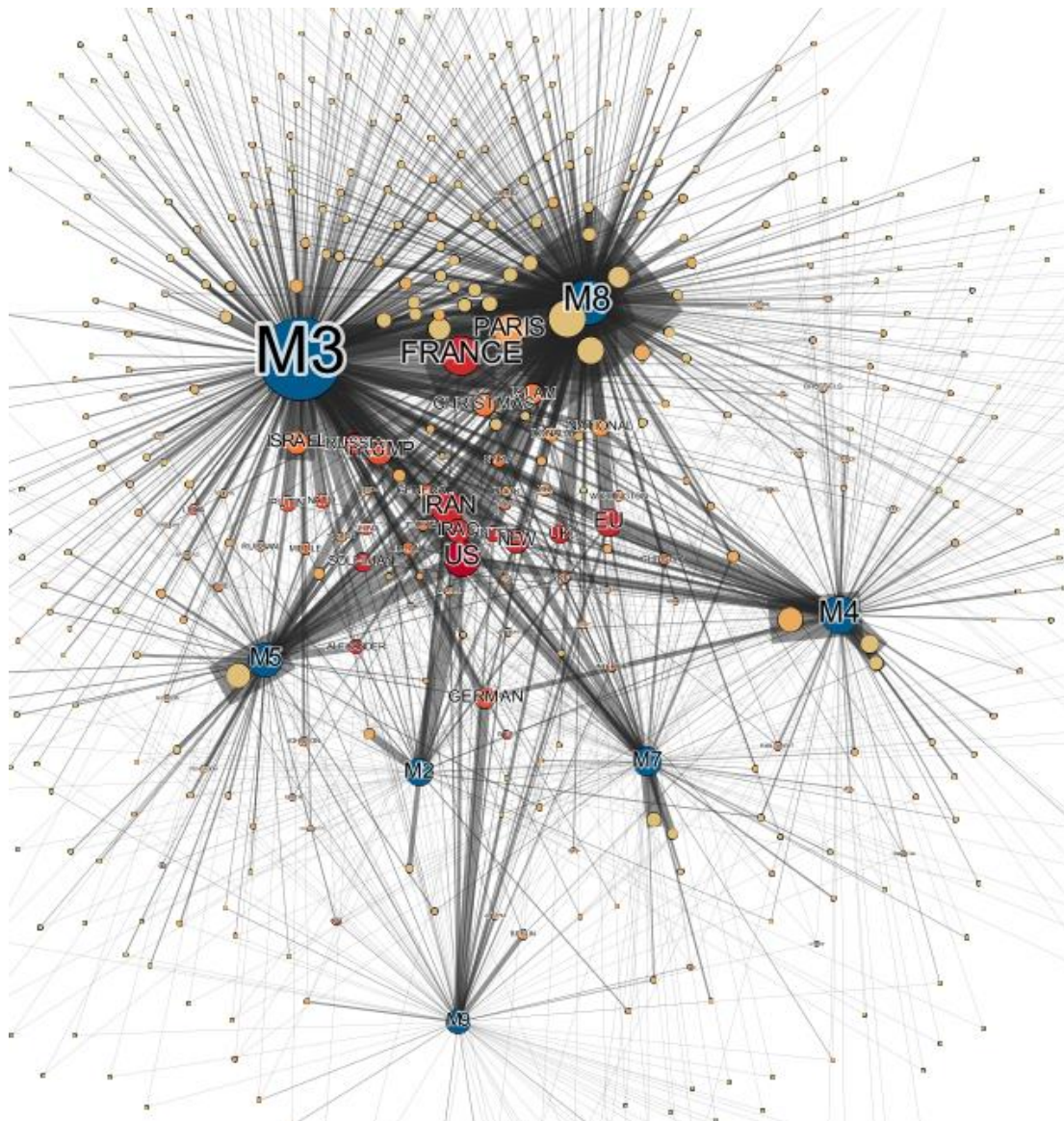
Le document 2 offre une représentation visuelle simplifiée des « relations dynamiques » (*linking behavior*) pour les neuf organisations médiatiques (appelée M1-9) de cette analyse. Cet indicateur présente la manière dont les différents sites internet référencent mutuellement leurs contenus et publications. Nous avons compté 37 liens vers des noms de domaine externes : 23 d'entre eux sont utilisés exclusivement par une organisation, et 5 des 14 restants le sont largement par plusieurs organisations médiatiques (l'un d'entre eux était YouTube par exemple). Sur ces 5, trois sont liés à une autre de ces neuf organisations médiatiques. En conséquence, la figure qui émerge montre des niveaux d'interconnexions assez éparés. Après classification, ce document permet de voir que les contenus les plus orientés vers la Russie restent groupés ensemble, et demeurent clairement séparés des amas proches de l'extrême-droite.



Document 2 : Analyse simplifiée de réseau de « relations dynamiques ».

³ Le dictionnaire *Larousse* définit une URL comme une «[a]dresse qui précise la localisation d'une ressource Internet en indiquant le protocole à adopter, le nom de la machine, le chemin d'accès et le nom du fichier. »

Une deuxième stratégie d'analyse, portant sur le contenu des publications cette fois, a été appliquée à cette base de données. A la différence du couplage lâche des liens URL, se concentrer sur les publications permet de faire ressortir des similitudes bien plus notables. En effet, 38 hashtags et entités étaient mentionnées dans les publications de cinq organisations médiatiques ou plus, et dix entités par sept organisations ou plus. Il s'agissait alors de « US », « FRANCE », « IRAN », « UE », « IRAK », « NOUVEAU », « RUSSIE », « UK », « SOLEIMANI » et « ALEXANDRE ». Le document 3 est une représentation visuelle de ces résultats. Les organisations médiatiques apparaissant en bleu ; les autres nœuds sont des éléments textuels représentés du jaune au rouge en fonction du nombre d'organisations les mentionnant, la taille des nœuds dépendant du nombre total de mentions. Ici, les entités textuelles mentionnées par une seule organisation ont été retirées pour permettre une lecture plus facile.



Document 3 : Une visualisation du réseau à partir des contenus.

En interprétant ces résultats, nous remarquons que les deux ensembles principaux (Russie, extrême droite) se tournent vers des sources médiatiques différentes alors même qu'ils discutent de sujets et de problèmes similaires. Pour cet article, il est intéressant de noter que si les campagnes de désinformation soutenues par l'extrême droite et la Russie utilisent des

écosystèmes médiatiques séparés, elles gravitent autour d'un certain nombre de sujets proches. Cette nuance permet de relativiser notre compréhension originelle de la nature des liens entre le Kremlin et les mouvements européens d'extrême droite. S'il y a des exemples évidents de soutien direct et matériel hors-ligne entre eux, chacun possède un paysage médiatique propre dans l'espace informationnel.

Adoption et adaptation pour la vie politique nationale

Grâce à la discussion précédente, on peut noter deux modes notables de communication utilisés par l'extrême droite et les acteurs soutenus par l'Etat russe afin de parvenir à leurs fins. Le premier gravite autour de la communication d'informations délibérément détournées et trompeuses. C'est l'archétype de la campagne de désinformation. Mais, parfois, l'information n'est pas fautive en elle-même ; en publiant des contenus que l'on préférerait voir rester de l'ordre du privé, un impact ou un avantage politique notable peut être obtenu. C'est ce que nous avons appelé une « opération informationnelle d'influence et d'interférence » (OIII). Le concept d'opération informationnelle est bien établi dans les études historiques de la Guerre froide, de l'espionnage et des méthodes soviétiques de propagande. Toutefois, comme le montre Schneier [2019], il ne permet pas de bien représenter la manière dont des activités analogues se déroulent dans l'environnement informationnel contemporain grâce aux réseaux sociaux. Schneier utilise donc le concept d'« opération d'influence » qui omet d'autres aspects essentiels. Pour cette raison, nous préférons lier ces deux définitions dans le concept « d'opération informationnelle, d'influence et d'interférence », qui associe le mécanisme employé (information) aux deux effets recherchés (influence et interférence). Ce concept suppose que l'influence socio-psychologique n'est pas le seul effet recherché : des actions matérielles et tangibles plus directes sont incluses dans l'idée « d'interférence ». En effet, pour comprendre comment les innovations stratégiques et tactiques poussées par les groupes d'extrême droite et par les agences soutenues par la Russie sont devenues courantes et répandues – durant les campagnes électorales notamment – il faut prendre en compte les campagnes de désinformation ainsi que les OIII.

On retrouve la meilleure illustration de ce modèle dans l'étude internationale conduite par Woolley et Howard [2019] qui recense les méthodes d'utilisation de la propagande informatique à travers un nombre croissant de pays. On retrouve d'autres preuves en soutien à cette interprétation dans les bases de données publiées par Twitter au cours des deux dernières années recensant les suspensions de comptes par pays pour « actions inauthentiques coordonnées ». Ces données sont résumées dans le tableau 1 ci-dessous. Même si certains comptes sont contrôlés de l'extérieur, nous pouvons supposer que la plupart des comptes ciblent le pays concerné..

PAYS D'ORIGINE	DATE DE PUBLICATION TWITTER	NOMBRE DE COMPTES
Chine	Juillet 2019	5241
Équateur	Avril 2019	1019
Iran	Octobre 2018	770
	Janvier 2019	2320
	Juin 2019	4779
Russie	Octobre 2018	3613
	Janvier 2019	416
	Juin 2019	4
Arabie saoudite	Avril 2019	6

Espagne	Avril 2019	259
Émirats arabes unis (+ Égypte)	Mars 2019 Avril 2019	4248 271
Venezuela	Janvier 2019	1960

Tableau 1 : Comptes Twitter récemment identifiés et fléchés pour « actions inauthentiques coordonnées », classés par pays d'origine.

A première vue, le tableau n'indique que le nombre de comptes concernés et le pays qui, selon Twitter, a entrepris de publier de la désinformation, en violation des conditions d'utilisation. On peut cependant penser que ces bases de données ne rassemblent que les activités les plus maladroitement déguisées. Elles permettent malgré tout d'observer la croissance et la prévalence de la désinformation, qui devient presque « normale » dans la vie politique et sociale contemporaine.

Des preuves plus qualitatives soutiennent par ailleurs cet argument. Ainsi, le suivi du référendum sur le Brexit et des élections générales suivantes a révélé la fabrication et la distribution de mésinformation (involontairement trompeuse) et de désinformation (volontairement trompeuse) dans le débat politique par des acteurs de tous bords. Parmi les exemples les plus parlants, nous pouvons noter : la promesse inscrite sur les bus de la campagne Vote Leave que 350 millions de livres pourraient être investis dans le NHS⁴ ; des idées conspirationnistes quant au responsable « réel » du meurtre de la députée Jox Cox ; l'utilisation « sélective » des sondages et la création de pamphlets ressemblant à de grands quotidiens connus par les Libéraux-démocrates ; et la publicité par Jérémy Corbyn, de documents issus des négociations commerciales UK-US et « divulgués » deux semaines avant les élections – des documents qui semblent avoir été piratés et distribués par un acteur (toujours inconnu) soutenu par l'Etat russe.

Une étude de cas estonienne

L'idée que les techniques et tactiques de désinformation, ancrées dans des rivalités géopolitiques, s'inscrivent de plus en plus dans la conduite de la politique interne est illustrée par des données collectées en Estonie. Cette étude de cas montre également la complexité des programmes respectifs de l'extrême droite et de l'Etat russe, ainsi que les tensions entre eux.

Depuis quelques années, un certain nombre de pays de l'ancien espace soviétique subissent une campagne continue de propagande, conduite ouvertement mais également insidieusement par des médias soutenus par la Russie et différents acteurs sur les réseaux sociaux. Elle se concentre sur trois discours centraux. L'objectif est de recouvrer une influence grandissante sur la gouvernance de ces pays en les détournant notamment du projet européen et de l'adoption des valeurs et institutions plutôt démocrates et libérales. Ces trois discours centraux sont, dans les grandes lignes :

1. Le nazisme baltique : une assertion récurrente affirme que les citoyens baltes sont historiquement très sympathiques aux idées et aux croyances nazies et, même si cette sympathie est désormais moins ouverte, elle perdure néanmoins.
2. Les discriminations contre les minorités ethniques russes : des affirmations pointent constamment du doigt une discrimination systématique contre les citoyens d'ascendance russe ou d'origine russophone, à la différence des populations « de souche ».

⁴ Le National Health Service (NHS) est le système de sécurité sociale britannique [N.d.T]

3. Les Etats en faillite : s'entrecroisant avec les deux discours précédents, cette idée soutient que les structures institutionnelles de ces pays sont si fragiles que leur intégrité fondamentales s'affaiblit avec le temps et qu'en conséquence, ils finiront probablement par s'effondrer.

Le cas estonien est particulièrement intéressant parce que le gouvernement a énormément investi dans la promotion d'une réputation nationale de progrès informatique et de compétences numériques. L'Estonie a promu le potentiel transformatif de l'e-gouvernement, probablement bien plus que les autres pays de la région (NDLR : voir l'article de Léa Ronzaud dans ce numéro).

A la manœuvre, on retrouve le Parti populaire conservateur d'Estonie, un petit parti communément appelé EKRE qui sait se faire entendre et gagne régulièrement en puissance. Le parti et son mouvement de jeunesse – le Sinine Äratus – souhaitent promouvoir « des valeurs nationales et une vision conservatrice du monde »⁵ même si le Conseil européen des relations internationales (ECFR) le décrit comme fortement « nationaliste, xénophobe, anti-libéral et eurosceptique »⁶. Leurs processions à la torche célébrant le nationalisme ont été assimilées aux marches « à la torche tiki » des partisans de Donald Trump à Charlottesville.⁷ Ils rejettent l'Occident mondialisé et ses institutions, et demandent une identité nationale forte, homogène, d'Europe de l'Est pour le peuple estonien. Cette identité doit embrasser l'héritage finno-ougrien partagé par les alliés hongrois, finlandais et polonais. Mais, si les valeurs proposées sont cohérentes avec nombre d'idées promues par la Russie, l'EKRE s'oppose catégoriquement à l'ancienne puissance occupante et se trouve même en conflit direct avec elle sur des questions telles que la frontière orientale et l'enseignement du russe dans les écoles du pays.

Jusqu'à récemment, l'EKRE était un élément extrême à la lisière du paysage politique estonien, alors que le pays était gouverné par une coalition sociale-démocrate depuis 2016. Mais lors des élections parlementaires de 2019, l'EKRE a plus que doublé son score et, malgré la controverse, est entré dans la nouvelle coalition gouvernementale. S'il a évidemment profité d'une vague de bons scores pour les partis populistes à travers l'Europe, la visibilité et le succès de l'EKRE en Estonie doivent également beaucoup à un réseau en ligne et hors-ligne très strictement coordonné. Dans la période préélectorale, il a été activé pour (i) confronter et attaquer publiquement ses opposants avec un discours désinformant, et (ii) profiter efficacement de la peur des Estoniens d'une stabilité nationale, d'une identité et de valeurs nationales réellement menacées par l'immigration et le libéralisme social.

Les enquêtes d'un quotidien national ont révélé durant la campagne électorale que des membres de la branche jeune du parti ont utilisé Facebook pour créer de faux comptes et ainsi « troller » leurs opposants politiques.⁸ Ces comptes étaient liés car chacun utilisait une variation du nom « Valter ». Ils publiaient régulièrement des commentaires incendiaires sur la presse en ligne et utilisaient Facebook Messenger pour viser les groupes LGBT et pro-égalité dont les réunions publiques étaient également sujettes à intervention. Le chef de Sinine Äratus de l'époque, Ruuben Kaalep, était engagé dans cette action sous le nom de « Bert Valter ». Ce réseau d'alter-egos de Valter était très actif et très efficace dans la création de groupes sur Facebook, de memes et de vidéos utilisant l'humour pour renforcer leur discours « à la vue de tous ». Lorsque

⁵ <https://sininearatus.ee/pohikiri/>

⁶ https://www.ecfr.eu/article/commentary_the_rise_of_estonias_radical_right_to_engage_or_not_to_engage

⁷ <https://www.telegraph.co.uk/news/2019/03/03/estonias-far-right-ekre-party-threaten-election-upset/>

⁸ <https://news.postimees.ee/6501755/ekre-sees-no-problem-with-trolling>

le journal a rendu cette activité publique, le chef de l'EKRE (aujourd'hui ministre de l'intérieur du gouvernement) a cherché à normaliser ces actions, en expliquant :

Je ne vois rien de critiquable, rien de criminel ici. Ce n'est rien de moins qu'une réaction face à une opération informationnelle menée par les médias traditionnels et qui est toujours en cours. Qui y-a-t-il de dommageable si une personne exprime ses opinions avec trois comptes Facebook différents ?

En réponse à ces révélations, d'autres soutiens de l'EKRE se sont mobilisés pour mener une contre-campagne numérique, en adoptant le hashtag #istandwithvalter et en visant les publications du quotidien sur Facebook avec des commentaires indiquant simplement « ekre ».

On peut également noter, dans la continuité de cet article, que l'EKRE et sa campagne numérique exploitaient une fracture sociale particulière ici (tout comme les médias étatiques russes) avec un sentiment anti-réfugiés qui grandissait alors que l'Estonie devait signer le Pacte migratoire de l'UE. Les statistiques affichaient une exigence d'accueil de réfugiés très faible pour l'Estonie, et presque la moitié des réfugiés du quota européen était déjà sur le territoire. Mais l'EKRE a rapidement et ostensiblement mobilisé ses soutiens pour manifester⁹ devant le Riigikogu (le siège du parlement estonien, *N.d.T*) et un Pacte qui, selon eux, menaçait la souveraineté de l'Estonie, une assertion que la présidente Kaljulaid a décrite comme « hystérique, mensongère, et blessante ».¹⁰ La pression incessante en ligne et hors-ligne de l'EKRE a miné la stabilité du gouvernement, en le poussant près de la démission. Finalement, cette pression a réussi à bloquer l'adoption du Pacte migratoire par l'Estonie et a placé cette question au cœur du débat public au moment des élections générales quatre mois plus tard.

Cette petite étude de cas permet de constater certaines subtilités et nuances qui existent dans les activités numériques des groupes de l'extrême droite et dans celles des entités soutenues par l'Etat russe. Certaines études ont tendance à présenter les intérêts des deux groupes d'acteurs comme totalement compatibles, ce qui est faux. Mais, comme le montre le cas présent, même lorsque les dissonances sont évidentes, le résultat final peut être le même : affaiblir l'intégrité des institutions et des processus démocratiques libéraux.

Conclusion

Cet article a présenté trois arguments principaux. Tout d'abord, il y a des croisements clairs entre les intérêts et les valeurs idéologiques des mouvements européens d'extrême droite et de l'Etat russe, même s'ils ne doivent pas être exagérés. Ensuite, l'extrême droite et les agences associées à l'Etat russe sont toutes deux responsables d'innovations importantes dans la conduite des campagnes de désinformation et dans les OIII. Finalement, les tactiques et techniques de désinformation, de tromperie et de détournement de l'information introduites ici ont été largement adoptées et adaptées par des acteurs politiques nationaux qui les ont progressivement normalisées.

Il est évident aujourd'hui que l'espace informationnel a été profondément pollué par des activités numériques d'ingénierie de l'influence conduites par des groupes affiliés à l'extrême droite cherchant à propager leurs idées et leurs préjugés, ainsi que par des organisations soutenues par la Russie souhaitant accentuer les asymétries perçues dans les relations géopolitiques entre les pays. Mais les contributions et l'alignement de ces acteurs ne doivent

⁹ <https://news.err.ee/880019/ekre-anti-migration-pact-protest-gets-out-of-hand-ratas-condemns-violence>

¹⁰ <https://www.postimees.ee/6454823/president-kritiseerib-valitsust-nadal-aega-on-koetud-uhiskondlikku-husteeriat-valetatud-ja-haiget-tehtud>

pas être surestimés, comme nous l'avons montré plus haut. D'autres acteurs ont également apporté une contribution importante dans ces développements, des acteurs commerciaux comme Cambridge Analytica notamment.

Ce qui est tout particulièrement remarquable, c'est que ces développements ont été menés en parallèle, et à peu près au même moment, que la promotion du *nudging* (c'est-à-dire, de l'économie comportementale) par d'autres domaines et disciplines académiques [Halpern 2015]. Le *nudging* implique l'utilisation de techniques d'influence et de persuasion pour encourager les individus à prendre certaines décisions plutôt que d'autres, en leur présentant l'information d'une certaine manière et avec la volonté de promouvoir des résultats précisément favorables à toute la société. On retrouve ici une similitude claire avec les technologies politiques opérationnelles de l'Internet Research Agency et des acteurs d'extrême droite. Mais la différence principale est que les conséquences désirées sont bien plus bénignes. On pourrait même dire que les acteurs étudiés ici pratiquent un « *dark nudging* » - ils cherchent à « pirater » la cognition, les émotions et les biais de la psychologie sociale humaine ainsi que les possibilités offertes par le développement de technologies par lesquelles une part non négligeable de la communication interpersonnelle transite aujourd'hui.

Les trajectoires de développement décrites ci-avant sont particulièrement difficiles à aborder pour les gouvernements qui doivent y répondre en construisant des politiques publiques alors même que les activités en question empiètent sur les méthodes traditionnelles d'organisation des autorités étatiques. Les gouvernements démocratiques libéraux tendent à séparer le domaine de la politique intérieure de la politique étrangère. Il est par exemple plus aisé de surveiller et contrôler les traces de la communication des autres acteurs étatiques sur les réseaux sociaux que celles de ses propres citoyens. Le risque que représente la désinformation a évolué et induit des tensions et des dilemmes nouveaux : jusqu'où est-il acceptable de chercher à contrôler les nuisances que l'on attribue à la désinformation ? Au demeurant, cela accentue probablement le niveau d'anxiété des agences gouvernementales par rapport aux conséquences à long-terme d'un système social où la manière dont on prend connaissance de l'information – et le type d'information lui-même – est de plus en plus fragile et fragmenté.

L'histoire montre que l'organisation sociale de la réalité a été régulièrement et profondément façonnée et refaçonée par les progrès des technologies médiatiques et communicationnelles. Les réseaux sociaux ont été initialement célébrés pour leur pouvoir de démocratisation et les possibilités de libéralisation qu'ils apportaient. Mais il est de plus en plus évident que ces plateformes sont également porteuses de pratiques de manipulation de masse grâce au *dark nudging* à un niveau et rythme inégalités jusqu'ici. Pour Vaughan [1996], la « normalisation de la déviance » trouve une place lorsque devient routinier ce qui était auparavant perçu comme exceptionnel. C'est un épithète très approprié pour décrire ce qu'il se passe en ce moment.

Bibliographie

Bartlett, J., Birdwell, J., et King, M. (2010), « The Edge of Violence: A Radical Approach to Extremism », *DEMOS* pp.7-55

Benkler, Y., Faris, R., et Roberts, H. (2018), *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. New York: Oxford University Press.

Bogerts, L. et Fielitz, M. (2019), « “Do You Want Meme War?” Understanding the Visual memes of the German Far Right », dans : Maik Fielitz et Nick Thurston [eds] *Post-Digital Cultures of the Far Right: Online Actions and Offline Consequences in Europe and the US*. pp.137-154

Bozdag, E., Gao, Q., Houben, J., Warnier, M. (2014), « Does Offline Political Segregation Affect the Filter Bubble? An Empirical Analysis of Information Diversity for Dutch and Turkish Users », *Computers in Human Behaviour* Vol.41 No.1 pp.405-415

Caiani, M. et Parenti, L. (2013), « Extreme Right groups and the Internet: Construction of Identity and Source of Mobilization », *European and American Extreme Right Groups and the Internet*. Ashgate, Austria pp.83-112

Caiani, M. et Parenti, L. (2013), « The Organizational Structure of the (Online) Galaxy of the European and American Extreme Right », *European and American Extreme Right Groups and the Internet*. Ashgate, Austria pp.55-82

Davey, J. et Ebner, J. (2017), « The Fringe Insurgency: Connectivity, Convergence and Mainstreaming of the Extreme Right », *Institute for Strategic Dialogue* pp.3-30, disponible sur : https://www.isdglobal.org/wp-content/uploads/2017/10/The-Fringe-Insurgency-221017_2.pdf

Dawson, A. et Innes, M. (2019), « How Russia’s Internet Research Agency built its disinformation campaign », *Political Quarterly*, 90/2: 245-56.

Giles, K. (2019), *Moscow Rules: What Drives Russia to Confront the West*. London: Chatham House.

Goffman, E. (1963), *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates*. New York: Anchor Books.

Halpern, D. (2015), *Inside the Nudge Unit*. London: WH Allen.

Hodge, E. and Hallgrimsdottir, H. (2019), « Networks of Hate: The Alt-Right, “Troll Culture”, and the Cultural Geography of Social Movement Spaces Online », *Journal of Borderlands Studies* pp.1-18

Innes, M., Roberts, C., Preece, A. et Rogers, D. (2018), « Ten Rs of social reaction: Using social media to measure the post-event impacts of the murder of Lee Rigby », *Terrorism and Political Violence*. 3/3: 454-74.

Innes, M., Dobрева, D. et Innes, H. (2019), « Disinformation and digital influencing after terrorism: Spoofing, truthing and social proofing », *Contemporary Social Science*. <https://doi.org/10.1080/21582041.2019.1569714>

Innes, M. (TBP), « Techniques of disinformation: Constructing and communicating ‘soft facts’ after terrorism », *British Journal of Sociology*

Jamieson, K. (2018), *Cyberwar: How Russian Hackers and Trolls Helped Elect a President*. New York: Oxford University Press.

Kakutani, M. (2018) *The Death of Truth*. London: Harper Collins.

Laruelle, M. (ed.) (2015), *Euransianism and the European Far Right*. Lanham, Ma.: Lexington Books.

Manivannan, V. (2013), « Tits or GTFO: The Logics of Misogyny on 4chan's Random - /b/ », *The Fibreculture Journal* Issn 1449-1443 pp.109 – 132 disponible sur : <http://fibreculturejournal.org/wp-content/pdfs/FCJ-158Vyshali%20Manivannan.pdf>,

Manivannan, V (2012), « Attaining the Ninth Square: Cybertextuality, Gamification, and Institutional Memory on 4chan », *Enculturation*, disponible sur : <http://enculturation.net/attaining-the-ninth-square>

Manning, P. (2016), « Goffman and empirical research », *Symbolic Interaction*, 39/1: 143–52

Margetts, H., John, P., Hale, S., et Yassera T. (2016), *Political Turbulence: How Social Media Shape Collective Action*, Princeton: Princeton University Press

Mudde, C. (2000), « The Extreme Right Party Family », dans : *The Ideology of the Extreme Right* Manchester University Press, United Kingdom pp.2-24

Nagel, A. (2017), *Kill All Normies: Online Culture Wars from 4chan and Tumblr to Trump and the Alt-Right*, Zero Books

Pasquale, F. (2016) *Black-Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, Ma. Harvard University Press

Pomerantsev, P. (2019) *This is NOT Propaganda: Adventures in the War Against Reality*. London: PublicAffairs.

Preece, A., Spasić, I., Evans, K., Rogers, D., Webberley, W., Roberts, C. et Innes, M. (2018) « Sentinel: A codesigned platform for semantic enrichment of social media streams », *118 IEEE Transactions on Computational Social Systems*, 5/1: 118–131. D
Schneier, B. Foreign Affairs

Roberts, C., Innes, M., Preece, A. et Rogers, D. (2018) « After Woolwich: Analysing open source communications to understand the interactive and multi-polar dynamics of the arc of conflict », *British Journal of Criminology*. 58/2: 434-54.4

Schneier, B. (2019), « 8 ways to stay ahead of influence operations », foreignpolicy.com (12/08/19)

Service, R. (2019), *Kremlin Winter: Russia and the Second Coming of Vladimir Putin*. London: Pan Macmillan.

Tuters, M. (2019), « LARPing and Liberal Tears: irony, Belief and Idiocy in the Deep Vernacular Web », Fielitz, Maik., et Thurston, Nick. [eds] *Post Digital Cultures of the Far Right: Online Actions and Offline Consequences in Europe and the US Political Science* Vol.71. pp.47-49

Vaughan, D. (1996), *The Challenger Launch Decision: Risky Technology, Culture and Deviance at NASA*. Chicago: University of Chicago Press.

Woolley, S. et Howard, P. (2019), *Computational Propaganda: Political Parties, Politicians and Political Manipulation on Social Media*, Oxford: Oxford University Press.