ÉCOLE NATIONALE D'ADMINISTRATION PUBLIQUE

MAÎTRISE EN ADMINISTRATION PUBLIQUE

ENP7972T – MÉMOIRE

PRÉSENTÉ À

STÉPHANE ROUSSEL

Un cadre stratégique des opérations d'information de la Russie

PRÉPARÉ PAR

JULIEN LAUZON CHIASSON

LAUJ10068708

AOÛT 2019

TABLE DES MATIÈRES

I. Résumé

Ce mémoire traite des opérations d'information modernes de la Russie. Ces opérations visent à manipuler l'environnement informationnel d'une société pour influencer ses réponses socio-politiques dans la sphère internationale. La problématique est de déterminer le fonctionnement de ces opérations. Ce fonctionnement est certainement détaillé dans des politiques et des manuels d'instructions russes. Cependant, ces sources documentaires primaires sont inaccessibles dû à leur niveau de classification.

Ainsi, une recherche empirique, qualitative et inductive a été menée pour en établir la teneur en fonction des actions posées lors de ces opérations. En étudiant les gestes accomplis par les agents d'information russes, il est possible de conceptualiser leur mode de fonctionnement. Ce *modus operandi* est identifié comme étant une *stratégie*.

Une étude de cas a été menée en se basant sur huit opérations. Elles ont eu lieu dans les pays baltes en 2007, en Géorgie en 2008, en Ukraine en 2014, en Suède en 2014, au Royaume-Uni en 2016, aux États-Unis en 2016, en France en 2017 et en Allemagne en 2017. Les méthodes employées par les Russes ont été catégorisées en fonction d'un cadre théorique des formes de puissance dans le cyberespace développé par Joseph Nye. Cette catégorisation ainsi que la compréhension d'ensemble fournie par l'étude de cas ont permis de construire trois modèles structurels des opérations d'information russes.

Le premier modèle montre l'augmentation des niveaux d'intensité de ces opérations en fonction de quatre stratégies. Le deuxième montre les stratégies possibles de manipulation de l'information. Le troisième montre le cycle de déploiement des activités. Ces trois modèles rendent compte de la structure stratégique globale des opérations d'information de la Russie. Le résultat principal est ainsi de proposer une typologie descriptive permettant une meilleure analyse des opérations d'information russes.

Les recherches accomplies témoignent d'une pensée théorique Russe distincte au sujet de la guerre de l'information. Selon celle-ci, les conflits sont continuels en temps de paix comme en temps de guerre. L'information y est l'arme centrale des guerres modernes. L'espoir de ce mémoire est que la compréhension qui y est développée puisse appuyer une réponse efficace de nos sociétés face aux conflits informationnels contemporains.

II. Introduction

> Russian information operations are a decisive tool of state power rather than a supporting element. Uniquely, Russian leaders are significantly more likely to employ diplomatic, military, and economic tools in pursuit of informational objectives than other states' leaders.[1]
>
> - T.S. Allen et A.J. Moore

Les élections américaines de 2016 ont mise en lumière les tentatives d'ingérence de la Russie dans les processus démocratiques. La possibilité que Vladimir Poutine ait influencé significativement la décision des électeurs américains de choisir Donald J. Trump comme 45e président des États-Unis a causé un choc qui s'est reflété dans la production intellectuelle universitaire et gouvernementale. Comment une élection, la pierre d'assise des régimes démocratiques, peut-elle être vulnérable aux manipulations d'une puissance étrangère? Et pas n'importe quelle élection! Celle de la superpuissance mondiale, défenseur auto-proclamé du monde libre!

Le choc initial mène à une réalisation d'une plus grande probité intellectuelle : les États ont de tout temps tenté d'influencer les processus décisionnels de leurs compétiteurs. La séduction, les rumeurs, la tromperie et les mensonges ont servi l'arsenal des conquérants et des chefs d'État à travers l'histoire. Malgré cela, il y a quelque chose d'unique à notre époque qui rend ce phénomène particulier : internet. À aucun autre moment de l'histoire, l'information n'a circulé aussi rapidement et globalement que dans le monde contemporain. Les nouvelles technologies de l'information et de la communication (NTIC) ont permis de renouveler les techniques de manipulation des sociétés et la pensée politique peine encore à s'y ajuster. Le cyberespace étant un nouvel environnement de compétition entre les États, il faut tenter d'en comprendre la dynamique.

---

[1] T.S. Allen et J. Moore (2018), *Victory without Casualties: Russia's Information Operations*, Parameters, 48(1), p.59, https://ssi.armywarcollege.edu/pubs/parameters/issues/Spring_2018/9_Allen_VictoryWithoutCasualties.pdf

L'objet de ce mémoire est la stratégie de déploiement des opérations d'information modernes de la Russie. Celle-ci représente le mode de fonctionnement de ces opérations, la façon dont les techniques utilisées sont déployées par les dirigeants du Kremlin. Il s'agit donc d'un mémoire essentiellement descriptif permettant d'améliorer notre compréhension d'un phénomène méconnu.

Il est ainsi exclu de déterminer si ces opérations ont une influence significative ou non sur la prise de décision des acteurs. Il est suffisant de considérer que si Moscou mène ces opérations, alors les dirigeants russes doivent évaluer qu'elles en valent la peine. Par ailleurs, considérant ces opérations font partie du secret étatique, il est aussi exclu d'analyser au premier degré les discours, les entrevues et les opinions de ces dirigeants concernant celles-ci. Ces messages sont partis intégrantes de ces opérations. Ils camouflent et confondent à leurs sujets.

Ce qui sera analysé sont les actions posées. À partir de ces actions, il est possible de remonter aux concepts, principes et structures leurs ayant donnée naissance. Ceci afin d'éclairer la problématique générale suivante : comment ces opérations fonctionnent-elles? Si les États occidentaux veulent établir des politiques pour se prémunir contre ces influences négatives, il faut d'abord commencer par en comprendre le fonctionnement.

Il est en revanche problématique d'imputer des intentions à un acteur à partir d'action observées. En effet, ce mémoire n'étudie pas les discours (intentions énoncés), ni n'effectue d'entrevues avec les acteurs. La nature du sujet étant de telle sorte que les acteurs sont présumés avoir intérêt à cacher ou du moins ne pas dévoiler de façon véridique les informations auxquelles nous tentons d'accéder. Cela signifie qu'il y a une nuance importante à faire entre les intentions présumées à partir des actions observées et les intentions réelles. N'ayant pas accès directement aux intentions réelles, nous tentons de les identifier à partir des observations accessibles. Cependant il existe un fossé qui nous est infranchissable entre les deux. Nous ne pouvons donc évidemment pas affirmer avec certitude que ce qui se dégage de nos observations représente sans nuances la pensée du Kremlin. Il ne s'agit que de la meilleure estimation que l'auteur réussit à en faire, avec toutes les limitations que cela comporte.

III. Cadre Théorique – Les relations internationales et les conflits dans le cyberespace

> There is an enormous disconnect between the cyber realities of today and the theories of the twentieth century, which continue to guide national policy and international relations.[2]
>
> - Choucri et Goldsmith

a. Faiblesse des fondements théoriques

Les approches théoriques concernant le cyberespace sont peu développées dans le domaine des relations internationales et des études de sécurité. Depuis plus d'une décennie, de nombreux auteurs soulignent cette lacune. En 2006, Eriksson et Giacomello écrivaient que: « very few attempts have been made to apply international relations (IR) theory in analyzing the information revolution, an exercise which seems warranted both for the understanding of the impact of the information revolution on security and for the development of IR theory »[3]. Ils ajoutaient que la majorité de la documentation était orientée sur le développement de politiques avec peu d'ambitions de contribuer au développement théorique. Il existait alors un écart évident entre les impacts de la révolution de l'information et leur compréhension théorique.[4]

Durant les douze années suivantes, ce constat a été répété à de multiples reprises. En 2010, Manjikian disait encore que: « we do not yet possess a coherent definition or theory of cyber power. We do not know how it relates to other aspects of power relations between states […] in the international system. […] Few analysts have integrated these queries into larger international relations theory ».[5] Puis entre 2012 et 2018, Choucri,

---

[2] N. Choucri et D. Goldsmith (2012), *Lost in cyberspace: Harnessing the Internet, international relations, and global security*, Bulletin of the Atomic Scientists, 68(2), p.75, https://journals.sagepub.com/doi/pdf/10.1177/0096340212438696

[3] J. Eriksson et G. Giacomello (2006), *The Information Revolution, Security, and International Relations: (IR)relevant Theory?,* International Political Science Review, 27(3), p.222, https://journals.sagepub.com/doi/pdf/10.1177/0192512106064462

[4] *Ibid*, p.228 et 235.

[5] M. M. Manjikian (2010), *From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik,* International Studies Quarterly, 54, p. 382, https://academic.oup.com/isq/article/54/2/381/1795973

Goldsmith, Kello, Isnarti, Craig, Valeriano et Maness tiraient la même conclusion.[6] Ainsi, la compréhension théorique des impacts des nouvelles technologies de l'information et des communications (NTIC) sur les questions de sécurité et sur les relations internationales reste rudimentaire.

Parmi les auteurs qui ont approché cette problématique, deux grands courants se distinguent. D'un côté, des auteurs comme Kello et Cavelty croient que les grandes théories du 20e siècle sont possiblement inaptes à approcher les questions ouvertes par la révolution numérique. Selon Cavelty et Mauer « 'grand' theorising about security in the information age is neither possible nor feasible »[7]. Kello prend une position moins définitive en évoquant la possibilité que l'« interpretation of cyber phenomena involves analysis of a new body of experience that existing theories may be unable to clarify. »[8]

D'un autre côté, plusieurs auteurs affirment que les théories des relations internationales pourraient aider à mieux comprendre les nouveaux phénomènes dévoilés par les NTIC. Ainsi, selon Valeriano et Maness, « there is much the field can learn from the perspectives of IR theory »[9] De même, Manijikan croit que « an understanding of the

---

[6] N. Choucri et D. Goldsmith (2012), *Lost in cyberspace: Harnessing the Internet, international relations, and global security*, Bulletin of the Atomic Scientists, 68(2), p.73, https://journals.sagepub.com/doi/pdf/10.1177/0096340212438696

L. Kello (2013), *The Meaning of the Cyber Revolution: Perils to Theory and Statecraft*, International Security, 38(2), p.8, https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00138

R. Isnarti (2016), *A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War*, Andalas Journal of International Studies, 5(2), p.151, http://ajis.fisip.unand.ac.id/index.php/ajis/article/view/53/43

A. J.S. Craig et B. Valeriano (2018), « Realism and Cyber Conflict: Security in the Digital Age », dans D. Orsi, J.R. Avgustin et M. Nurnus (dir.), *Realism in Practice*, E-International Relations Publishing, p. 89, https://eprints.ncl.ac.uk/file_store/production/245064/D474E3F6-4CEE-45C9-AC88-BF59E19C0ADC.pdf#page=101

B. Valeriano and R. C. Maness (2018), « International Relations Theory and Cyber Security », dans C. Brown et R. Eckersley, *The Oxford Handbook of International Political Theory*, Oxford University Press, p.260.

[7] M. D. Cavelty et V. Mauer (2007), « The Role of the State in Securing the Information Age – Challenges and Prospects », dans M. D. Cavelty, V. Mauer et S. F. Krishna-Hensel (dir.), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*, Ashgate Publishing, p.158.

[8] L. Kello (2013), *The Meaning of the Cyber Revolution: Perils to Theory and Statecraft*, International Security, 38(2), p.7, https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00138

[9] B. Valeriano and R. C. Maness (2018), « International Relations Theory and Cyber Security », dans C. Brown et R. Eckersley, *The Oxford Handbook of International Political Theory*, Oxford University Press, p.269.

various [theoretical] lenses used to visualize cyberspace will help to better predict and analyze initiatives undertaken by all players within the cyberspace system. »[10]

Bien que les théories du 20e siècle puissent se révéler incapable d'incorporer une conception adéquate du cyberespace, il y a tout de même pour l'ensemble des auteurs précédemment cités « an evident need for scholars of international relations and security to contribute to the theoretical evaluation of the cyber revolution »[11].

Cette revue de la documentation théorique révèle trois constats importants.

1. Les fondations théoriques du cyberespace pour les relations internationales et les études de sécurité sont peu développées.
2. Il est possible que les grands cadres théoriques existants soient inadéquats pour conceptualiser les nouveaux phénomènes du cyberespace.
3. Il est malgré tout nécessaire de théoriser le domaine du cyberespace et ses enjeux de sécurité.

b. Tentatives de théorisation du cyberespace

Un des enjeux de sécurité du cyberespace est celui des opérations d'information modernes. La modernisation de ces opérations est attribuable à la part grandissante qu'est venue jouer le cyberespace dans nos vies quotidiennes depuis le tournant du millénaire. Dans le contexte de cette recherche, la question suivante se pose : quels cadres théoriques ou concepts permettent de rendre compte de l'intégration par les États des outils du cyberespace à leurs opérations d'information ?

Le peu de théorisation associé à ce nouveau champ de recherche ayant déjà été établi, il est difficile de simplement appliquer un cadre théorique préexistant à ces

[10] M. M. Manjikian (2010), *From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik,* International Studies Quarterly, vol. 54, p. 398, https://academic.oup.com/isq/article/54/2/381/1795973
[11] L. Kello (2013), *The Meaning of the Cyber Revolution: Perils to Theory and Statecraft*, International Security, 38(2), p.8, https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00138

phénomènes. Par ailleurs, plusieurs auteurs ont émis une mise en garde sur la possible futilité d'appliquer les théories du 20e siècle aux nouveaux phénomènes du cyberespace.

Pour surmonter ces difficultés, Eriksson et Giacomello proposent comme solution de faire preuve de pragmatisme. Plutôt que de débattre au sujet duquel des courants dominants traditionnels peut le mieux rendre compte de ces phénomènes, il serait préférable de faire usage de complémentarité théorique, de pluralisme méthodologique, de généralisations contingentes et de tolérance entre diverses approches. Afin de surmonter le fossé entre la théorie et la pratique, il faudrait donc à la fois emprunter aux théories traditionnelles leurs outils les plus appropriés et s'inspirer des recherches orientées vers la pratique.[12] « With such a pragmatic approach applied to case studies and comparative analyses, it is possible to build a foundation upon which further theory building can be done, with an emphasis on middle-range theory and on conditional rather than universal generalizations. »[13]

Eriksson et Giacomello en donnent un exemple en exposant comment le réalisme, le libéralisme et le constructivisme peuvent chacun conceptualiser leur part de ces nouveaux phénomènes. Ainsi, le réalisme peut concevoir la guerre de l'information comme une continuité des formes classiques de la guerre psychologique, bien que sa perspective trop centrée sur l'État et le domaine militaire soit problématique. Le libéralisme saisit l'importance de la multiplication des acteurs non-étatiques et la vulnérabilité de l'interdépendance, mais son idéalisme lui permet difficilement de concevoir les formes plus néfastes de l'utilisation du cyberespace. Le constructivisme est approprié pour analyser les affrontements symboliques, rhétoriques et identitaires. Il peut concevoir la guerre de l'information comme une guerre dans laquelle l'identité d'un État-nation est en jeu. Toutefois, ce cadre conceptualise moins clairement l'impact des outils informatiques sur les capacités matérielles des États.[14]

---

[12] J. Eriksson et G. Giacomello (2006), *The Information Revolution, Security, and International Relations: (IR)relevant Theory?,* International Political Science Review, 27(3), p.236, https://journals.sagepub.com/doi/pdf/10.1177/0192512106064462

[13] *Ibid*, p.236.

[14] *Ibid*, p.228-236.

Manjikian emprunte une approche semblable en comparant comment les théories traditionnelles peuvent rendre compte de cette nouvelle situation. Selon elle, les possibilités du cyberespace apparaissent complètement différemment selon chacune des approches. Elles offrent des prédictions différentes sur les possibilités de conflits et de coopération. Ainsi, alors que des approches libérales mettaient l'accent sur l'utopie d'un territoire international, communautaire et partagé, des approches réalistes se penchaient sur les questions de la protection de ce territoire, sur la puissance de ce lieu et sur une guerre des idées.[15] Alors que les débuts d'internet ouvraient la porte à un certain idéalisme, l'apparition depuis de la cybercriminalité, du cyberterrorisme, des guerres de l'information et des attaques informatiques renforcent la philosophie réaliste du cyberespace.

Le réalisme pourrait alors sembler bien positionné pour approcher cet objet. Pourtant, selon Craig et Valeriano, même s'il reste un cadre pertinent pour identifier certains enjeux de sécurité important et offrir un aperçu des caractéristiques durable du système international, « realist theories about conflict often fall substantially short in explaining the unique dynamics of cyber conflict. »[16] Tout comme Kello, Craig et Valeriano encouragent « the development of new theories based on empirical observation or the deductive logics of the cyber domain rather than automatically falling back on realist theories that were developed to explain kinetic forms of warfare. »[17]

Depuis les premiers appels à une approche pragmatique et à l'application flexible des théories dominantes pour expliquer les conflits dans le cyberspace, aucun cadre de recherche traditionnel ne s'est imposé pour offrir un modèle clair de la dynamique d'utilisation des cybers capacités par les acteurs étatiques et non-étatiques Pour Craig et Valeriano, « with further empirical research, we can gain more precise understandings of key issues »[18]. Même sans cadre théorique traditionnel, des concepts préexistants peuvent

---

[15] M. M. Manjikian (2010), *From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik,* International Studies Quarterly, vol. 54, p. 387 et 398, https://academic.oup.com/isq/article/54/2/381/1795973

[16] A. J.S. Craig et B. Valeriano (2018), « Realism and Cyber Conflict: Security in the Digital Age », dans D. Orsi, J.R. Avgustin et M. Nurnus (dir.), *Realism in Practice*, E-International Relations Publishing, p. 94, https://eprints.ncl.ac.uk/file_store/production/245064/D474E3F6-4CEE-45C9-AC88-BF59E19C0ADC.pdf#page=101

[17] *Ibid*, p.95

[18] *Ibid*, p.95

permettent d'orienter la recherche empirique. En appliquant le pragmatisme de Eriksson et Giacomello, une tolérance et une flexibilité dans l'approche théorique permet de collecter plus de données, de construire des études empiriques et d'améliorer notre compréhension du phénomène pour solidifier les approches théoriques du cyberespace qui peinent à prendre forme.

Le réalisme et le libéralisme offrent tout de même un point de départ. Le cyberspace ne fait pas exception de la continuité historique des relations entre les États en ce qu'il reproduit des relations de compétition et de coopération dans un nouvel espace. Les relations du cyberespace s'entremêlent avec les mondes physique et psychologique pour influencer la dynamique et l'équilibre de puissance du système international. Ces nouveaux enjeux de sécurité offrent donc une continuité dans la philosophie qui sous-tend les rapports étatiques, bien qu'ils soient en rupture quant à l'environnement et aux dynamiques de ces relations.

Une approche particulière s'est toutefois dégagée comme étant particulièrement bien adaptée à notre objet. Ainsi, afin de conceptualiser ces nouveaux phénomènes, « one of the few serious efforts to merge new realities into core theoretical concepts is the work of Joseph Nye on "cyberpower" »[19].

c. Le *cyberpower* selon Nye

Nye conceptualise le cyberespace selon deux plans. D'abord au plan physique, il regroupe l'ensemble des infrastructures et des ressources humaines permettant la transmission des informations. Au plan virtuel, il s'agit d'un flot d'informations en mouvement. Le *cyberpower* peut ainsi être défini comme les ressources liées à la création, au contrôle et à la communication d'informations électroniques basées sur les ordinateurs.[20] Toutefois, selon une perspective comportementale, « cyberpower is the ability to obtain preferred outcome through use of the electronically interconnected information resources

[19] L. Kello (2013), *The Meaning of the Cyber Revolution: Perils to Theory and Statecraft*, International Security, 38(2), p.12-13, https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00138
[20] J. S. Nye (2011), *The Future of Power*, New York, Public Affairs, p.123.

of the cyberdomain. »[21] Ce qui distingue les opérations d'information modernes de leur version traditionnelle est l'utilisation du cyberespace pour atteindre leurs objectifs. Les objectifs peuvent à la fois être dans le cyberespace et hors de celui-ci, considérant sa structure à double niveau. De plus, une conception comportementale la puissance dans le cyberespace permettra de mieux comprendre le fonctionnement des opérations d'information. En effet, ces opérations ont pour objectif une influence comportementale.

La puissance fonctionne différemment dans le cyberespace que dans le monde matériel. Les règles de son utilisation échappent partiellement aux concepts employés précédemment pour réguler l'usage de la puissance par les États.[22] Par contre, les actions humaines et leur logique se maintiennent et se poursuivent dans ce nouvel environnement. C'est ainsi que Nye se permet d'appliquer sa catégorisation du spectre du *soft* au *hard power* à la fois aux instruments informationnels et physiques, Ceux-ci peuvent avoir une influence à l'intérieur ou à l'extérieur du cyberespace (voir **l'annexe 1** pour le tableau de Nye en exemple). Les instruments physiques et virtuels peuvent donc être utilisés selon une logique de *soft* ou de *hard power* et leurs impacts peuvent se faire sentir dans l'espace physique comme dans le cyberespace. Par exemple, les attaques de déni de service distribué (DDoS) sont une forme de *hard power* dans le cyberespace, déployé avec des instruments informationnels. À l'opposé, des manifestations populaires pour dénoncer de ''mauvais'' utilisateurs du cyberespace (comme peuvent en être accusé certains États ou des compagnies collaborant avec eux) sont un instrument physique faisant usage du *soft power* pour affecter le monde hors du cyberespace.[23]

Nye présente aussi une deuxième méthode de catégorisation de la puissance dans le cyberespace. Il y a ici trois aspects à la puissance (voir **l'annexe 2** pour le tableau de Nye en exemple).

---

[21] *Ibid*, p.123.

[22] *Ibid*, p.124-126

Par ailleurs, ce n'est pas la première fois qu'une invention technologique vient bouleverser les règles régissant l'utilisation de la puissance. À titre d'exemple, l'arme nucléaire a eu pour effet de transformer l'art et les règles de la guerre au 20e siècle.

[23] *Ibid*, p.126-128.

1. Lorsqu'un acteur A induit à un acteur B de faire un choix qu'il n'aurait pas fait autrement.
2. Lorsqu'un acteur A limite les choix d'un acteur B en excluant des stratégies de B.
3. Lorsqu'un acteur A transforme les préférences d'un acteur B de telle sorte que certaines stratégies ne sont même pas considérées.

Chacun de ces aspects de la puissance peut employer le *soft* ou le *hard power*. À un extrême du spectre, insérer un virus informatique est un exemple de *hard power* du premier aspect de la puissance. À l'autre extrême, les campagnes virtuelles visant à stimuler les sentiments patriotiques est un exemple de *soft power* du troisième aspect de la puissance.[24]

Alors que la première catégorisation met l'accent sur les instruments (informationnels ou physiques) utilisés pour agir dans ou sur le cyberespace, la deuxième catégorisation met l'accent sur les stratégies des acteurs selon leur type d'influence. Ces deux modèles sont complémentaires dans la mesure où les acteurs utilisent à la fois des instruments et des stratégies. La particularité des opérations d'informations modernes est que de nouveaux instruments ont mené au développement de nouvelles stratégies. Ces deux modèles aideront à rendre compte de la dynamique stratégique de ces nouveaux instruments de puissance.

d. Le *soft power* et ses critiques

Nye aborde la puissance sous un angle comportemental, plutôt qu'uniquement selon la possession d'une quantité de ressources et de capacités. Il la définit comme étant « the ability to influence the behavior of others to get the outcomes one wants. »[25] Cette habilité est naturellement magnifiée par une grande quantité de ressources disponibles, mais elle se distingue plus précisément par l'aptitude à employer ces ressources pour obtenir les résultats voulus. Considérant que l'objectif de cette recherche est d'analyser une stratégie étatique (c'est-à-dire une méthode pour guider l'utilisation des ressources d'un État), une approche comportementale de la puissance convient bien à l'angle théorique.

[24] *Ibid*, p.129-131
[25] J. S. Nye (2004), *Soft Power*, New York, Public Affairs, p. 2.

Le *soft power* se définit comme « getting others to want the outcome that you want ».[26] C'est une forme de puissance qui coopte et attire plutôt que de contraindre. À l'inverse, le *hard power* est « the ability to make others do what you want »[27]. Il s'agit d'une façon de commander à un acteur d'adopter un comportement qu'il n'aurait pas effectué sans l'ombre de la menace ou de la récompense. Le *hard power* influence ce que les acteurs font, alors que le *soft power* influence ce que les acteurs veulent. Ce qui distingue ces deux formes de puissance est une question de degrés. Il s'agit d'un spectre d'actions allant de la contrainte à l'attirance.[28]

Le concept du *soft power* a toutefois essuyé nombre de critiques. Christopher Layne en fait un résumé dans son chapitre intitulé « The unbearable lightness of soft power »[29].

1. Les mécanismes causaux selon lesquels le *soft power* est supposé fonctionner sont flous. Quelle est la chaîne causale par laquelle il affecte le résultat des politiques? Nye attribue le fonctionnement du *Soft Power* à la légitimité, c'est-à-dire à l'action d'un État selon des normes collectivement partagées et respectées. Ceci est lié à des politiques multilatéralistes et au cautionnement par des institutions internationales. Ce comportement, attirant le respect et l'admiration des peuples et des nations, les incites à suivre l'acteur. Toutefois, est-ce que le *soft power* est une variable indépendante ou simplement une façon de parler pour traiter des variables précédemment mentionnées? S'il s'agit d'une variable indépendante, alors comment entre-t-elle en relation avec les normes, les institutions internationales et le multilatéralisme?[30]

2. La théorie de Nye se rapproche dangereusement de d'autres théories des relations internationales (institutionnalisme, paix démocratique, constructivisme). Ainsi, quelle

[26] *Ibid*, p.5
[27] G. Zahran et L. Ramos (2010), « From hegemony to soft power », dans I. Parmar et M. Cox (dir.), *Soft Power and US Foreign Policy: Theoretical, historical and contemporary perspectives*, New York, Routledge, p.13.
[28] J. S. Nye (2004), *Soft Power*, New York, Public Affairs, p.5-7.
[29] C. Layne (2010), « The unbearable lightness of soft power », dans I. Parmar et M. Cox (dir.), *Soft Power and US Foreign Policy: Theoretical, historical and contemporary perspectives*, New York, Routledge, p.51 à 82.
[30] *Ibid,* p.54-55.

est la différence entre le *soft power* et ces théories? De plus, quelle est la valeur ajoutée de ce concept par rapport à ces théories?[31]

3. La définition du *soft power* est inconstante et a été graduellement étendue pour inclure de plus en plus d'éléments. Le concept était originellement une forme d'attirance pure (sans contraintes ou incitatifs), puis il a ultérieurement englobé certains outils économiques et même certaines formes de la puissance militaire.[32]

4. Le *soft power* se conçoit comme un processus en deux étapes qui, en premier, vise à affecter l'opinion publique d'un État pour que, en deuxième, le gouvernement réponde à cette influence par la modification de ses politiques. Toutefois, un argument s'opposant à l'opérationnalisation du concept est que « [the] public opinion does not make foreign policy, the state's central decision makers do. And there is little reason to believe that public opinion affects their calculations significantly. »[33]

e. Réponses de Nye à ses critiques

Nye a répondu à ces critiques par les clarifications suivantes :

1. Le *soft power* est un concept relationnel. Il est une influence relative aux diverses préférences des acteurs. L'action des acteurs dans le cadre de normes, de culture et d'institutions peuvent avoir des effets différents selon les individus touchés. Le *soft power* sert plutôt à analyser le type de comportement des acteurs en relation les uns aux autres dans des environnements affectés par des normes, des cultures et des institutions.[34]

[31] *Ibid*, p.54.
[32] *Ibid*, p.54-55.
[33] *Ibid*, p.56.
[34] J. S. Nye (2010), « Responding to my critics and concluding thoughts », dans I. Parmar et M. Cox (dir.), *Soft Power and US Foreign Policy: Theoretical, historical and contemporary perspectives*, New York, Routledge, p.218.

2. Le *soft power* est un concept analytique et non une théorie. Ce concept peut concorder avec des perspectives réalistes, libérales ou constructivistes. Il s'agit d'une forme de puissance et il est donc normal qu'elle puisse s'appliquer à l'ensemble des théories des relations internationales. À l'époque de l'introduction du concept, le néoréalisme avait réduit les conceptions de la puissance uniquement à la forme matérielle. Le *soft power* permettait de réintroduire dans les théories des relations internationales, les formes plus immatérielles de puissance.[35]

3. Cette critique confond l'action des États avec les ressources à leur disposition. Plusieurs types de ressources peuvent servir à exercer un *soft power*, mais cela ne signifie pas que le *soft power* réfère à n'importe quel type de comportement.[36]

4. Il est vrai que plusieurs gouvernements dans plusieurs contextes sont faiblement contraints par l'opinion publique. Toutefois les élites d'un gouvernement sont parfois directement influencées par des idées étrangères. C'était le cas de Gorbachev et de sa politique de la *perestroika* et du *glastnost* qui ont été influencées par des idées américaines provenant d'Alexander Yakovlev. De la même façon, des gouvernements peuvent être contraints dans leur action par la force de l'opinion publique. C'était le cas lorsqu'en 2003, les responsables turces ne pouvaient pas laisser passer sur le territoire l'armée américaine se dirigeant vers l'Iraq. Une prise de position pro-américaine aurait signifié de grands problèmes pour le gouvernement vis-à-vis d'une opinion publique résolument anti-américaine.[37]

Pour résumer, ce que mentionnent en général l'ensemble des critiques est la nécessité de clarifier le concept. « A call that has been acknowledged and repeated by Nye himself. »[38]

[35] *Ibid*, p.219-220.
[36] *Ibid*, p.219
[37] *Ibid*, p.218-219.
[38] E. Lock (2010), « Soft power and strategy », dans I. Parmar et M. Cox (dir.), *Soft Power and US Foreign Policy: Theoretical, historical and contemporary perspectives*, New York, Routledge, p.32.

f. Les limites de l'usage du concept de *soft power* pour les opérations d'information

Pour combiner l'usage du *hard* et du *soft power*, Nye a formulé le terme de *smart power*. Ce dernier permet d'intégrer les deux formes de puissance dans une stratégie de politique étrangère. Cette intégration des deux concepts vise plus spécifiquement à influencer la direction de la politique étrangère américaine en suggérant des stratégies incluant à la fois les capacités de contraindre et d'attirer.[39]

Cela est tout à fait compréhensible dans la pensée stratégique américaine, mais cette conceptualisation des stratégies de puissance est-elle applicable aux stratégies de tous les États, notamment aux États autoritaires comme la Russie? Certes la Russie a son propre *soft power*. Sa culture, son idéologie et ses institutions ont leur force d'attraction.[40] Par contre, Nye conçoit le spectre du *hard* et du *soft power* comme un continuum se différenciant par une question de degrés.[41] Entre ces deux extrêmes, il existe une zone grise où le *hard* et le *soft power* se confondent. Dans cette zone grise, est-il possible qu'une stratégie puisse permettre d'attirer en contraignant et de contraindre en attirant? Les opérations d'information ne sont pas une forme de contrainte, personne n'est forcé d'adopter les informations qui leur sont proposées. Il ne s'agit pas non plus d'une forme d'attraction pure, alors que la tromperie et les mensonges ne sont pas une méthode pour inspirer le respect et l'admiration. Elles s'inspirent des méthodes du *soft power* comme la diplomatie publique, la diffusion de valeurs communes et le dialogue dans des institutions partagées[42]. Elles sont une forme de puissance en ce qu'elles visent à inciter une cible à vouloir ce que l'acteur veut. Par contre, il n'est pas clair si la volonté de la cible y est libre, comme le voudrait le *soft power,* ou si l'acteur est contraint, comme le voudrait le *hard power*.

---

[39] J. S. Nye (2010), « The future of soft power in US foreign policy », dans I. Parmar et M. Cox (dir.), *Soft Power and US Foreign Policy: Theoretical, historical and contemporary perspectives*, New York, Routledge, p.9.

[40] Par exemple la littérature russe, le nationalisme et l'église orthodoxe peuvent avoir une puissance d'attraction.

[41] « Hard and soft power are related because they are both aspects of the ability to achieve one's purpose by affecting the behavior of others. The distinction between them is one of degree, both in the nature of the behavior and in the tangibility of the resources. »

- Joseph Nye (2004), *Soft Power*, New York, Public Affairs, p.7.

[42] Internet et les réseaux sociaux peuvent être conçus comme des institutions partagées.

Par exemple, l'intrusion de force dans des serveurs informatiques pour voler de l'information compromettante est une forme de contrainte. L'accès à l'information a été forcé contre la volonté de la cible. Cependant, lorsque ces informations sont diffusées dans la sphère publique et que les individus consomment librement cette information, ils peuvent être attirés par celle-ci et cela les incites à vouloir ce que l'acteur à l'origine de cette stratégie voulait (soit éloigner les électeurs d'un candidat politique). Contrairement au *soft power,* la cible ne veut pas ce que l'acteur voulait car elle est inspirée, admirative ou respectueuse de celui-ci. L'acteur a manipulé l'information de telle sorte que la cible agisse conformément à ce que son environnement informationnel dicte en relation avec ses valeurs et ses croyances. Une partie de cette manipulation se fait sous la contrainte et une partie se fait par attirance. Nye avait proposé le concept de *smart power* pour rendre compte des stratégies combinant des méthodes de *soft* et de *hard power*. Par contre, la stratégie des opérations d'information semble bien éloignée des intentions originelles de Nye lorsqu'il proposait d'user du « smart power by once again investing in the global public goods – providing things that people and governments in all quarters of the world want but cannot attain in the absence of leadership by the largest country. »[43]

g. La stratégie de *soft power* des gouvernements autoritaires : le *sharp power*

À l'origine de son analyse du *soft power* à l'ère numérique, Nye faisait deux observations qui se présentaient comme des prédictions d'espérance. Malheureusement, certains gouvernements autoritaires viendront modifier ces prédictions.

Premièrement, pour Nye, une des implications « [of] this global information age is that the relative importance of soft power –cultural and ideological appeal- will also increase, because soft power rests on credibility. »[44] Selon lui, les pays qui augmenteront leur *soft power* sont:

[43] J. S. Nye (2010), « The future of soft power in US foreign policy », dans I. Parmar et M. Cox (dir.), *Soft Power and US Foreign Policy: Theoretical, historical and contemporary perspectives*, New York, Routledge, p.10.
[44] J. S. Nye (2002), *The Information Revolution and American Soft Power*, Asia-Pacific Review, 9(1), p.69, https://www.tandfonline.com/doi/pdf/10.1080/13439000220141596?needAccess=true

> « 1. Those whose dominant culture and ideas are closer to prevailing global norms (which now emphasize liberalism, pluralism, and autonomy);
>
> 2. Those with the most access to multiple channels of communication and thus more influence over how issues are framed;
>
> 3. Those whose credibility is enhanced by their domestic and international performance. These dimensions of power in an information age suggest the growing importance of soft power in the mix of power resources, and a strong advantage to the United States. »[45]

Deuxièmement, selon Nye, l'écart entre les ressources du cyberespace détenues par les acteurs étatiques et non-étatiques se rétrécit. Ainsi, « what is distinctive about power in the cyberdomain is […] that the gap between state and nonstate actors is narrowing in many instances. »[46]

Le portrait d'inspiration libérale du *soft power* dans le cyberespace de Joseph Nye est donc un monde dans lequel la distribution de la puissance se démocratise parmi les acteurs non-étatiques et où le *soft power* avantage les pays aux cultures et idées conformes aux normes internationales, ceux ayant le plus grand accès aux canaux de communication et dont la crédibilité est renforcée par leur bonne performance domestique et internationale. Tous ces éléments donneraient un avantage aux États-Unis. Ainsi, l'importance d'inspirer et d'attirer sera renforcée par le développement du cyberespace et en contrepartie celle du contrôle diminuera. En particulier, le contrôle de l'information par les États diminuera. En 2002, Nye prédisait alors que:

> Central surveillance is possible, but governments that aspire to control information flows through control of the Internet face high costs and ultimate frustration. Rather than reinforcing centralization and bureaucracy, the new information technologies have tended to foster network organizations, new types of community, and demands for different roles for government.[47]

Cette vision du cyberespace s'est partiellement réalisée. Certains gouvernements ont souffert de cette libéralisation de l'information lors des vastes soulèvements populaires du printemps arabe ou par suite des fuites d'informations confidentielles sur l'armée

---

[45] *Ibid*, p.70.
[46] J. S. Nye, *The Future of Power*, New York, Public Affairs, p.132.
[47] J. S. Nye (2002), *The Information Revolution and American Soft Power*, Asia-Pacific Review, 9(1), p.61, https://www.tandfonline.com/doi/pdf/10.1080/13439000220141596?needAccess=true

américaine en Irak et celles sur les programmes de surveillance de la National Security Agency (NSA).

Toutefois, une évolution différente et parallèle a eu lieu avec les méthodes de contrôle et d'influence du cyberespace par certains régimes autoritaires, dont les principaux sont la Chine et la Russie.[48] Ces régimes ont d'un côté centralisé le contrôle national du cyberespace et de l'autre ont développé leurs canaux de communication pour tenter de transformer les normes internationales et affecter négativement la crédibilité des démocraties libérales. Ceci leur permet d'exploiter à leur avantage une version différente et plus maline du *soft power*.

Le *sharp power* est un concept introduit dans un rapport du *National Endowment for Democracies* pour conceptualiser l'influence grandissante des régimes autoritaires. Ainsi, « authoritarian influence efforts are "sharp" in the sense that they pierce, penetrate, or perforate the information environments in the targeted countries. »[49] Cette influence ne vise pas à gagner le cœur et l'esprit des populations, mais plutôt à contrôler subtilement l'information. En utilisant notamment la censure, la manipulation, le mensonge, la propagande et la tromperie, ces régimes ont redéfini à leur avantage le sens du *soft power*. En appliquant les trois critères que Nye avait définis comme garant de l'augmentation du *soft power* d'un pays à l'ère numérique, ils ont augmenté la portée, la vitesse et la qualité de la propagande et des méthodes d'espionnage classiques. La capacité de percer et de pénétrer un environnement informationnel pour y introduire à large échelle des messages qui auront un impact sur la prise de décisions est la stratégie propre au *sharp power*.[50]

[48] R. Rohozinski et R. Deibert (2010), *Liberation vs. Control: The Future of Cyberspace*, Journal of Democracy, 21(4), p.43-57, https://www.journalofdemocracy.org/articles/liberation-vs-control-the-future-of-cyberspace/

[49] C. Walker et J. Ludwig (2017), *Sharp Power: Rising Authoritarian Influence*, National Endowment for Democracies, p.13, https://www.ned.org/wp-content/uploads/2017/12/Sharp-Power-Rising-Authoritarian-Influence-Full-Report.pdf

[50] *Ibid,* p.13.

h. Le *sharp power* et ses critiques

Suite à la formulation du *sharp power* pour rendre compte de la stratégie d'influence des gouvernements autoritaires, Nye a publié un article pour argumenter que le *sharp power* est en réalité une forme de *hard power*. Il affirma ainsi: « sharp power, the deceptive use of information for hostile purposes, is a type of hard power. »[51] Il ajoute que la distinction entre le *soft power* et le *sharp power* est subtile et difficile à discerner. Cadrer des informations selon un angle particulier est une caractéristique du *soft power*, mais quand ce cadrage se transforme en tromperie, alors, selon Nye, cela devient un cas de *sharp power*. Lorsqu'un acteur limite les choix volontaires d'un sujet, cela est une forme de contrainte et donc de *hard* ou de *sharp power*. La qualité de transparence, d'ouverture et de libre choix fait office de limite. Ainsi, quand un acteur présente ouvertement son point de vue (même s'il s'agit d'un régime autoritaire), il fait usage de *soft power*, mais lorsqu'il se dissimule sous de fausses apparences pour présenter une information trompeuse ou censure certaines opinions, alors il limite la capacité du sujet de discerner le sens des enjeux et fait donc usage de *hard power*.[52]

La question à savoir si le *sharp power* est une nouvelle version du *soft power* ou simplement une forme de *hard power* est abordée différemment par Xin Liu. Selon elle, « sharp power is neither soft nor hard power—it is the product of an unskilled mixing of the two ». « It *is* something different from the three established concepts of soft, hard and smart power. »[53] Elle précise que les intentions de *soft power* de tous les États sont bonnes, mais qu'elles peuvent être déformées par l'application de *hard power*. Ainsi, si le *smart power* est un mélange habile de *soft* et de *hard power*, le *sharp power* serait un mélange malhabile des deux.[54] Elle aborde cette question sous l'angle de la diplomatie publique chinoise et il faut donc prendre un peu de recul par rapport à l'idée que le *sharp* power ne serait simplement qu'une stratégie malhabile. Toutefois, cet argument est intéressant en ce qu'il

[51] J. S. Nye (2018), *How Sharp Power Threatens Soft Power*, Foreign Affairs, https://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power
[52] *Ibid.*
[53] X. Liu (2018), *What Sharp Power? It's nothing but "unsmart" power*, USC Center of Public Diplomacy, https://www.uscpublicdiplomacy.org/blog/what-sharp-power-it%E2%80%99s-nothing-%E2%80%9Cunsmart%E2%80%9D-power
[54] *Ibid*.

permet d'expliquer l'usage changeant des mêmes outils avec des intentions différentes entre des stratégies de *smart* et *sharp power*.

En appelant à une nouvelle stratégie de *smart power*, Wilson III reconnaît que la puissance « increasingly rests on a nation's capacity to create and manipulate knowledge and information. »[55] Toutefois, il ne fait pas de distinction entre son utilisation par les démocraties ou les régimes autoritaires. Il définit le « smart power as the capacity of an actor to combine elements of hard power and soft power in ways that are mutually reinforcing such that the actor's purposes are advanced effectively and efficiently »[56] Selon sa définition, il ne fait aucun doute qu'un acteur pourrait employer le *smart power* d'une façon très différente de celle promu par ses partisans aux États-Unis.

Pour Walker Ludwig, le *sharp power* est né du besoin d'un nouveau terme pour définir le phénomène des stratégies d'influence des régimes autoritaires de la Chine et de la Russie. Nye mentionne avec raison que le *sharp power* ne présente pas une nouvelle définition de la puissance, mais rend compte du passage flou d'activités de *soft power* à des activités de *hard power*. Liu précise par ailleurs que le *sharp power* n'est pas une nouvelle forme de puissance, mais plutôt une combinaison stratégique différente du *soft* et du *hard power.* Wilson III expose une conception du *smart power* qui pourrait très bien s'appliquer au *sharp power* chinois ou russe. Des études ont par ailleurs fait usage du concept de *sharp power* pour rendre compte des opérations d'influence chinoise à l'étranger[57] et à Taiwan[58]. Ces deux études ont comme point commun qu'elles n'étudient pas une théorie de la puissance, mais une stratégie de son utilisation.

Théoriquement, affirmer que le *sharp power* serait une conceptualisation de la puissance supplémentaire au *soft power* de Nye est difficile à défendre. Percer et pénétrer un environnement informationnel peut se faire par la coercition comme par l'attraction. Le

---

[55] E. J. Wilson III (2008), *Hard Power, Soft Power, Smart Power*, The American Academy of Political and Social Science, 616(1), p.112, https://journals.sagepub.com/doi/pdf/10.1177/0002716207312618
[56] *Ibid*, p.115.
[57] J. M. Cole (2018), *THE HARD EDGE OF SHARP POWER: Understanding China's Influence Operations Abroad*, Macdonald-Laurier Institute, https://macdonaldlaurier.ca/files/pdf/20181022_MLI_China's_Influence_(Cole)_PAPER_WebreadyF.pdf
[58] G. Read (2019), « SHARP POWER, YOUTH POWER, AND THE NEW POLITICS IN TAIWAN », Dans J. Golley, L. Jaivin, P. J. Farrelly et S. Strange (dir.), *Power*, ANU Press, p.179-184, https://www.jstor.org/stable/j.ctvfrxqkv.21

sharp power se pose plus clairement comme pendant du *smart power*. En effet, il représente une stratégie d'utilisation différente du *soft* et du *hard power.* La définition du *sharp power* peut simplement s'appliquer aux opérations d'information : « pierce, penetrate, or perforate the information environments in the targeted countries. »[59] Cette définition clarifie l'acte performé, mais omet d'en définir le but. Elle se révèle donc incomplète. Toutefois, elle ouvre la porte à une version autoritaire des stratégies de *smart power* conçues dans les pays démocratiques.

i. Implications théoriques pour ce mémoire

Cette exploration du cadre théorique a commencé par révéler les manquements dans les théories des relations internationales et des études de sécurité concernant le cyberespace. Par la suite, l'application qu'a effectuée Nye de sa théorie de la puissance au cyberespace a servi de base à une catégorisation des actes accomplis dans le cyberespace. Toutefois, le concept stratégique du *smart power*, qui visait à appliquer cette théorie dans le domaine de la politique étrangère, s'est révélé insatisfaisant pour concevoir les opérations d'information des régimes autoritaires. Par ailleurs, le concept de *sharp power*, qui a eu un certain écho pour définir le phénomène, se dévoile ne pas être l'équivalent du *soft power* mais plutôt une combinaison particulière des techniques relevant à la fois du *soft* et du *hard power*.

La théorie de Nye et les débats entourant le *sharp power* indiquent quoi chercher. Il faut regarder à la fois du côté des méthodes du *soft* et du *hard power*, les catégoriser et montrer comment elles transitent l'une dans l'autre pour percer un environnement informationnel et y injecter un contenu malveillant. En ce sens, elles agissent précisément à l'image des virus informatiques. Elles pénètrent, cachées, les défenses d'un système pour y déposer un programme qui collectera, injectera ou détruira des données.

Au final, le cadre théorique peut apporter deux choses à cette recherche.

[59] C. Walker et J. Ludwig (2017), *Sharp Power: Rising Authoritarian Influence*, National Endowment for Democracies, p.13, https://www.ned.org/wp-content/uploads/2017/12/Sharp-Power-Rising-Authoritarian-Influence-Full-Report.pdf

- Premièrement, il permet de classifier les données selon les deux tableaux proposés par Nye (voir annexes 1 et 2). Une classification en fonction des formes de puissance (*soft* ou *hard*), selon le domaine d'application (interne ou externe au cyberespace) et aux instruments utilisés (physiques ou informationnels) permettra de catégoriser les méthodes grâce auxquelles sont effectué les opérations d'information.[60] Une seconde catégorisation, selon trois aspects de la puissance, permettra de clarifier les stratégies employées par les opérations d'information. Quels aspects de la puissance sont dominants dans ces opérations? Vise-t-on plutôt à forcer un acteur à agir d'une certaine façon, à exclure certaines stratégies de ses choix possibles ou à influencer ses préférences de telle sorte que certains choix ne soient pas considérés?[61]

- Deuxièmement, la revue de la documentation théorique nous a montré les limites de la théorisation existante dans ce domaine. Il n'existe pas de modèle établi des actions étatiques dans le cyberespace (et encore moins des opérations d'information). Cela empêche l'emploi d'une méthodologie déductive visant à vérifier des hypothèses. Toutefois, certaines avancées conceptuelles et des recherches empiriques ont permis d'approcher les phénomènes et d'y jeter un éclairage particulier. Ainsi, le concept de *sharp power* révèle que les opérations d'information sont un mélange de méthodes de *soft* et de *hard power*. Une compréhension de cette stratégie devra donc exprimer comment ces deux formes de puissance sont intégrées conjointement.

Par ailleurs, plusieurs des auteurs précédemment mentionnés dans ce chapitre ont exprimé l'importance de poursuivre les études empiriques dans ce champ de recherche, de même que celle de la systématisation et de la conceptualisation des données. C'est à cet appel que le présent mémoire répond. Sa méthodologie sera donc inductive, conformément au faible avancement des théories dans ce champ et au besoin exprimé par les chercheurs.

[60] Cette classification correspond au tableau de l'annexe 1.
[61] Cette classification correspond au tableau de l'annexe 2.

IV. Méthodologie – comment dévoiler la stratégie des opérations d'information?

> De façon presque unanime, on reconnait la valeur de l'étude de cas pour les recherches exploratoires. La science est souvent mal armée pour comprendre les nouveaux phénomènes, comme les dernières formes de cybercriminalité. Pour de telles réalités, les méthodes qualitatives et l'étude de cas présentent des qualités indéniables : (…) on peut « découvrir » et mieux comprendre des phénomènes nouveaux ou difficiles à mesure.[62]
>
> - Simon N. Roy

> When the degree of secrecy is intense and well institutionalized, then the policy domain and objects themselves become blurry and opaque.[63]
>
> - William Walters

a. Objectif et question de recherche

L'objectif de cette recherche est de proposer une compréhension conceptuelle de la stratégie des opérations d'information russes. La problématique que nous souhaitons clarifier est : Comment concevoir l'intégration des techniques de manipulation de l'information en une tentative d'influence organisée? Cette organisation (ou coordination) des techniques est ici nommée *stratégie*. Tel que le démontrera la revue documentaire, les techniques des opérations d'information (fausses nouvelles, *trolls*, *bots,* hameçonnage, etc.) ont été étudiées par de nombreux chercheurs. En revanche, les connaissances sont pauvres concernant les concepts et les modèles permettant de rendre compte de l'organisation de ces opérations. De plus, la compréhension de ces opérations est compliquée dû à la nature de celles-ci. Puisqu'il s'agit d'une activité secrète de l'État, les sources directes détaillant la structure et le mode de fonctionnement de ces opérations sont inaccessibles, car classifiées à un haut niveau. Toutefois, comme l'explique Walters, « [many] classified programs and covert operations are not deep secrets so much as known unknowns. We know they exist but what most of us know is very partial and uneven. »[64]

---

[62] S. N. Roy (2016), « L'étude de cas », dans B. Gauthier et I. Bourgeois (dir.) *Recherche sociale: De la problématique à la collecte de données*, 6e édition, Québec, Presses de l'Université du Québec, p.199.
[63] W. Walters (2015), *Secrecy, publicity and the milieu of security*, Dialogues in Human Geography, 5(3), p.288, https://journals.sagepub.com/doi/10.1177/2043820615607766
[64] *Ibid*, p.289.

En réunissant ces connaissance partielles et inégales, un portrait plus global de ces opérations pourra être constitué.

b. Recherche exploratoire

La question de recherche est de type exploratoire. Il s'agit d'une « question de recherche ouverte portant sur un thème peu connu, en exploration (…) et dont le chercheur n'est pas en mesure d'établir un portrait à partir des connaissances existantes. »[65] La méthode de preuve privilégiée est l'étude de cas. Elle « permet la description en profondeur et l'enclenchement d'un processus inductif. »[66] L'étude de cas servira donc à collecter les informations nécessaires à une compréhension approfondie du phénomène. Cette collecte est qualitative en ce qu'une description des phénomènes sera faite. Cette approche inductive permettra d'abstraire de la diversité des événements décrits une structure détaillant les possibilités conceptuelles de déploiement de ces opérations. Ainsi, tel que le présente Gauthier, le but est de déterminer si « la situation existante peut nous apprendre quelque chose que l'on puisse formuler ensuite au moyen d'un modèle temporaire de représentation de la réalité? »[67]

La force de l'étude de cas est de permettre d'aborder des nouveaux phénomènes peu connus et difficilement quantifiables. En explorant ces événements, il sera possible d'établir des constantes, des tendances et des récurrences qui solidifieront une compréhension de l'usage du cyberespace comme lieu de lutte informationnelle.

c. L'étude de cas – ses limites et sa portée

Cette étude de cas est de type phénoménal.[68] Elle porte sur un phénomène pouvant se présenter dans diverses sociétés à divers moments. Les opérations d'information sont utilisées par toutes les grandes puissances. Chacune d'elles obéissent à une doctrine particulière qui rend leur stratégie unique. La portée de cette étude de cas ne s'applique

[65] B. Gauthier (2016), « La structure de la preuve », dans B. Gauthier et I. Bourgeois (dir.) *Recherche sociale: De la problématique à la collecte de données*, 6e édition, Québec, Presses de l'Université du Québec, p.163.
[66] *Ibid*, p.163.
[67] *Ibid*, p.164.
[68] S. N. Roy (2016), « L'étude de cas », dans B. Gauthier et I. Bourgeois (dir.) *Recherche sociale: De la problématique à la collecte de données*, 6e édition, Québec, Presses de l'Université du Québec, p.199.

donc pas aux opérations des autres pays, ni à celles de l'Union Soviétique (bien qu'elles en soient inspirées) et elle ne peut pas prétendre prédire avec précision les opérations d'information russes futures. En revanche, cette étude s'inscrit dans un continuum permettant de suivre l'évolution du phénomène et d'établir un point de départ pour maintenir une veille des opérations à venir.

L'étude de cas portera ainsi sur les opérations d'information russes en Occident entre 2007 et 2017. La Russie moderne et sa prédécesseure, l'Union Soviétique, ont une longue tradition d'ingérence dans les sociétés occidentales. Les traces de l'utilisation de l'information comme arme y remonte au moins jusqu'à l'époque tsariste avec la publication des *Protocoles des sages de Sion*[69]. Suite à la chute de l'Union Soviétique, son influence en Occident décline avec l'affaiblissement de l'État et de son idéologie. On retrouve malgré tout un retour à ces opérations sur la scène intérieure durant les deux guerres de Tchétchénie, en 1994-1996[70] et 1999-2000[71]. La forme moderne de ces opérations débute toutefois en 2007 avec la première utilisation publique des armes du cyberespace à des fins politiques en Europe. Cette opération avait lieu en Estonie, alors que la relation entre les États-Unis et la Russie s'empirait avec la crise de l'installation d'un système de défense antimissile américain en Pologne. Les opérations d'information russes ont connu une croissance jusqu'à leur apogée durant les élections américaines de 2016. Elles se sont poursuivies durant l'élection française de 2017 et ont entamées un léger déclin lors de l'élection suivante en Allemagne quelques mois plus tard. Ces opérations sont encore actives, bien qu'elles semblent présentement être retournées dans une phase de dormance.

Durant ces dix années, huit occurrences d'opérations d'information russes ont été sélectionnées : les pays baltes (Lettonie, Estonie et Lituanie) depuis la cyberattaque de 2007 en Estonie, la guerre de Géorgie en 2008, l'Ukraine depuis la révolution de l'*Euromaïdan* de 2014, la Suède à partir de 2014, le référendum de 2016 sur le *Brexit* au Royaume-Uni, l'élection présidentielle de 2016 aux États-Unis, l'élection présidentielle de

[69] Un manifeste antisémite russe datant de 1903 à l'origine exacte incertaine mais que certains chercheurs attribuent à Mathieu Golovinski, un représentant de la police politique du Tsar.
[70] R. Clogg (1997), *Disinformation in Chechnya: an anatomy of a deception*, Central Asian Survey, 16(3), p.425-430.
[71] G. P. Herd (2000), *The 'counter-terrorist operation' in Chechnya: 'Information warfare' aspects*, The Journal of Slavic Military Studies, 13(4), p.57-83.

2017 en France et l'élection fédérale de 2017 en Allemagne. D'autres opérations ont aussi eu lieu, par exemple en Italie et en Espagne (Catalogne). Toutefois, les 8 choisies l'ont été car elles sont à la fois les plus importantes géopolitiquement pour le Kremlin et elles ont été bien documentées par des chercheurs ou des gouvernements.

d. Validité de l'étendue sélectionnée

Les études de cas ont une tension méthodologique interne entre une validité interne et une validité externe.

> D'une part, d'aucuns diront que les études de cas sont subjectives et s'appuient sur des informations partielles et ***qui ne représentent pas toute la réalité du cas.*** (…) D'autre part – et c'est peut-être la critique la plus sérieuse -, on reproche à la méthode de se pencher sur des cas ***qui ne sont pas « représentatifs » de la population à laquelle ils appartiennent.***[72]

Pour répondre à la première critique, la solution est d'intensifier la quantité du détail des données constitutives du cas. En représentant avec le plus de précision possible le cas, la validité interne en sera augmentée. Pour ce faire, le cas doit être plus limité dans le temps et dans l'espace afin de pouvoir offrir une description très précise. Malheureusement, en offrant une description limitée mais précise, la validité externe en est affectée. Puisque l'échantillon est limité, il devient moins représentatif du phénomène dans son ensemble. La solution est alors d'étudier le cas plus largement en incluant l'ensemble des phénomènes constitutifs du cas. La tension provient de ce que la description intensive du détail et l'ampleur de l'échantillon entre en opposition en fonction des contraintes de temps et de ressources de la recherche.

Pour cette étude de cas, la décision a été prise de favoriser la validité externe. Plusieurs recherches ont été faites avec une forte validité interne sur des occurrences particulières aux États-Unis, en Suède, en Ukraine et ailleurs. En se basant sur leur validité interne, cette étude visera à être plus représentative du phénomène dans son ensemble. De cette façon, le modèle conceptuel dégagé sera plus représentatif de la structure globale des opérations d'information russes. En effet, une étude plus limitée (se concentrant par exemple seulement sur l'opération aux États-Unis), aurait été mieux supportée par de

[72] S. N. Roy (2016), « L'étude de cas », dans B. Gauthier et I. Bourgeois (dir.) *Recherche sociale: De la problématique à la collecte de données*, 6e édition, Québec, Presses de l'Université du Québec, p.200.

nombreux exemples détaillés, mais elle serait moins généralisable à l'ensemble de l'échantillon. La stratégie dégagée aurait été propre à une seule occurrence et non à l'ensemble. Considérant que les politiques et les doctrines sont formulées au niveau des hautes instances politico-militaires, une analyse de la stratégie doit pouvoir remonter à ce niveau en prenant une vue d'ensemble, semblable à celle des décideurs ayant formulées ces politiques. En sélectionnant un nombre élevé d'occurrences (8) dans l'étude de cas, la validité externe sera haussée, de même que la possibilité de généraliser l'analyse finale à la stratégie globale des opérations d'information russes.

e. Processus d'exploration

La revue documentaire permettra la mise en contexte de l'étude de cas en définissant ce qui est déjà connu sur les principes, les concepts, les outils et les buts des opérations d'information. Par la suite, l'étude de cas organisera les données recensées selon l'étendue précédemment définie. Finalement, l'analyse de ces données dévoilera les processus stratégiques (c'est-à-dire la structure conceptuelle suivie par les Russes lors d'une opération d'information) à l'aide des deux modèles théoriques de Nye et des observations révélées par l'étude de cas.

f. Note sur la terminologie et les définitions

Il existe une certaine confusion au sujet de la définition des concepts entourant les opérations d'information. Cette confusion n'est pas étrangère au fait qu'ils ont souvent des significations différentes en Occident et en Russie. La documentation reflète régulièrement cette désorganisation terminologique.

> In English, concepts such as information operations, command and control warfare, psychological operations, information security, cyberpower, influence operations, electronic warfare, military deception, cybersecurity, strategic communication, public diplomacy, cyber espionage, cyberwar etc. abound. To the professional, some of them have precise and well-defined meanings, some of them have become non grata, and some are just vague. (…) To the layman, the intricacies of these terms are even less transparent. In Russian, much the same is

true. Many different terms are used, sometimes in purportedly precise ways, more often not.[73]

La présente recherche est orientée autour de trois concepts centraux. Ils seront compris selon les définitions suivantes :

Guerre de l'information : Niveau d'analyse le plus général. Il saisit la compréhension conceptuelle du rôle crucial, pour certains théoriciens russes, de l'information dans les conflits du 21e siècle. Il s'agit d'une traduction directe des concepts russes de « informatsionnoe protivoborstv » et « informatsionnaia voin », qui sont communément utilisés en Russie pour traiter de ce phénomène.[74]

Opération d'information : Dans le contexte de la guerre de l'information, une opération d'information est une action offensive menée sur un territoire spécifique dans le but d'influencer l'environnement informationnel à des fins politiques. En fonction de la doctrine militaire canadienne, le niveau opérationnel se situe entre le niveau stratégique (supérieur) et le niveau tactique (inférieur). Il est associé à l'échelle d'un pays ou d'une région regroupant quelques pays ou territoires de petite ou moyenne taille.[75]

Stratégie : L'organisation des opérations selon des principes généraux. Il s'agit de la structure des opérations tel qu'elles ont pu être conçues au niveau du commandement ou des dirigeants politiques. Elle réfère à la structure conceptuelle guidant les opérations.

« Strategy, in its broadest sense, is the art of devising and employing a plan or process to achieve an objective. At the national strategic level, strategy is the art and science of developing and employing the instruments of national power (…) in a synchronized and comprehensive fashion to secure national objectives. »[76]

[73] U. Franke (2015), *War by non-military means Understanding Russian information warfare*, Swedish Defence Research Agency (FOI), p.10, http://johnhelmer.net/wp-content/uploads/2015/09/Sweden-FOI-Mar-2015-War-by-non-military-means.pdf
[74] *Ibid*, p.10.
[75] Ministère de la Défense nationale (2009), *CFJP 01 Canadian Military Doctrine*, Gouvernement du Canada, p.1-3, http://publications.gc.ca/collections/collection_2010/forces/D2-252-2009-eng.pdf
[76] *Ibid*, p.3-2.

La distinction entre la propagande et la désinformation porte à confusion. La différence tient toutefois au cadrage (propagande) comparativement à la falsification intentionnelle (désinformation) d'une information. « It is the falsification or staged event accompanying the persuasive message that distinguishes disinformation from run-of-the-mill propaganda. »[77] Dans les faits, les organes de transmission russes diffusent le plus souvent à la fois de la propagande et de la désinformation.

Propagande : La propagation d'idées, d'opinions ou d'informations conforment à une vision du monde ou une idéologie afin d'influencer l'opinion publique. Les informations sont cadrées de sorte qu'elles favorisent le point de vue du propagandiste. « Ideas, facts, or allegations spread deliberately to further one's cause or to damage an opposing cause. »[78]

Désinformation : La transmission d'informations intentionnellement fausses dans le but de tromper un ou des acteurs à des fins politiques. « Disinformation comprises two parts: a forgery or fabrication, and the publicity that accompanies it to effectuate some psychological advantage for the originator of the disinformation. »[79]

[77] L. J. Martin (1982), *Disinformation: An instrumentality in the propaganda arsenal*, Political Communication, 2(1), abstract, https://www.tandfonline.com/doi/abs/10.1080/10584609.1982.9962747
[78] Merriam-Webster dictionary, *Propaganda*, https://www.merriam-webster.com/dictionary/propaganda
[79] L. J. Martin (1982), *Disinformation: An instrumentality in the propaganda arsenal*, Political Communication, 2(1), abstract, https://www.tandfonline.com/doi/abs/10.1080/10584609.1982.9962747

V. Revue documentaire – état de la question

> A new type of war has emerged, in which armed warfare has given up its decisive place in the achievement of the military and political objectives of war to another kind of warfare - information warfare.[80]
>
> - V. Kvachkov[81]

Les opérations d'information sont aisément aussi vieilles que la guerre elle-même. Le résumé par Griffith de la philosophie de la guerre de Sun Tzu témoigne bien de l'importance de la manipulation de l'information pour les anciens stratèges :

> The master conqueror frustrated his enemy's plans and broke up his alliances. He created cleavages between sovereign and minister, superiors and inferiors, commanders and subordinates. His spies and agents were active everywhere, gathering information, sowing dissension, and nurturing subversion. The enemy was isolated and demoralized; his will to resist broken. Thus without a battle his army was conquered, his cities taken and his state overthrown.[82]

Le 21e siècle a toutefois apporté une révolution technologique majeure avec l'intégration des outils numériques à la majorité de nos méthodes de communication et de transfert d'informations. Cette évolution technologique a profondément transformé la conduite des opérations d'information. L'environnement informationnel s'étant transformé, les outils et la pensée stratégique s'y sont adaptés.

a. Conception russe de la guerre de l'information (GI)

Giles présente la conception que se fait la Russie de la guerre de l'information (GI) comme étant très différente de celle des pays de l'Organisation du traité de l'Atlantique

---

[80] Citation de: V. Kvachkov (2004), Спецназ России (Russia's Special Purpose Forces), Voyennaya Literatura, http://militera.lib.ru/science/kvachkov_vv/index.html dans K. Giles (2016), *Handbook of Russian Information Warfare*, NATO Defense College, p.3. http://www.ndc.nato.int/news/news.php?icode=995

[81] « Vladimir Kvachkov is a former GRU officer, whose "theory of special operations", including information operations, has reportedly been adopted as the basis for Russian military instructional and training materials. » - *Ibid*., p.3.

[82] Sun Tzu, *The Art of War*, traduction et introduction par Samuel B. Griffith, Oxford University Press, 1971, p.39.

Nord (OTAN). La doctrine militaire américaine déploie des opérations d'information en soutien et conjointement avec les autres efforts opérationnels. Ainsi, « the Secretary of Defense now characterizes IO [Information Operations] as the integrated employment, **during military operations**[83], of IRCs [Information Related Capabilities] in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own. »[84] De plus, pour la défense américaine, « there is significant interdependency between IO and CO [Cyberspace Operations]. »[85] Selon cette doctrine, les opérations dans le cyberspace peuvent agir en soutien aux opérations d'information et les deux domaines opérationnels sont fortement interconnectés, bien que distincts.[86]

Par opposition, « ''cyber'' as a separate function or domain is not a Russian concept. »[87] La délimitation des activités dans et hors du cyberspace entre traiter, attaquer, perturber ou voler de l'information est étrangère à la pensée russe. Leurs opérations d'information ne se concentrent pas essentiellement sur le soutien aux opérations militaires. Les cyberattaques, l'exploitation de l'information et les chaînes d'information comme *Russia Today* sont tous des outils inter-reliés de guerre de l'information.[88]

La sécurité dans le cyberespace est conçue différemment de la stratégie américaine. Pour la Russie, il n'est pas possible de déterminer que « the [National Cyber] Strategy's success will be realized when cybersecurity vulnerabilities are effectively managed through identification and protection of networks, systems, functions, and data (…) [and] activity that is contrary to responsible behavior in cyberspace is deterred through the imposition of costs »[89]. Cette conception ne peut pas s'appliquer à la stratégie russe car

[83] Nous mettons l'emphase.
[84] U.S. Department of Defense (2014), *Joint Publication 3-13 Information Operations*, United States Government, p.ix, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf
[85] U.S. Department of Defense (2018), *Joint Publication 3-12 Cyberspace Operations*, United States Government, p.ix, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150
[86] U.S. Department of Defense (2014), *Joint Publication 3-13 Information Operations*, United States Government, p.II-9, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf
[87] K. Giles (2016), *Handbook of Russian Information Warfare*, NATO Defense College, p.7, http://www.ndc.nato.int/news/news.php?icode=995
[88] *Ibid*, p.8.
[89] United States Government (2018), *National Cyber Strategy of the United States of America*, The White House, p.3, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

cette dernière ne fait pas de distinction entre la sécurité de l'information dans le cyberespace et la vie ''réelle''.[90] « Instead of cyberspace, Russia refers to "information space," and includes in this space both computer and human information processing, in effect the cognitive domain. »[91]

Pour approcher la conception russe de la guerre de l'information, il ne faut pas partir de la distinction entre le cyberespace et l'espace physique, ni des opérations d'information comme étant parallèles et complémentaires aux autres types d'opérations. Il faut plutôt concevoir la centralité du concept *d'information* comme déterminant l'intégration des outils dans une stratégie commune. « In the Russian conceptual framework, this information can be stored anywhere, and transmitted by any means – so information in print media, or on television, or in somebody's head, is subject to the same targeting concepts as that held on an adversary's computer or smartphone. »[92] Face à la révolution numérique, la Russie n'a pas tenté de définir un domaine d'activité distinct ayant sa propre stratégie. Elle a plutôt intégré les nouvelles méthodes aux activités préexistantes et a redéfini l'ensemble de sa stratégie autour de l'importance primordiale de l'information dans l'environnement opérationnel du 21e siècle. Pour Giles,

> The scope and potentiality of information warfare in the Russian conception should not be measured against more recent Western concepts of information operations, or information activities, and in particular it should not be confused with cyber operations. The Ukraine conflict has provided clear demonstrations of how Russia sees cyber activity as a subset, and sometimes facilitator, of the much broader domain of information warfare.[93]

b. Domaines russes de la guerre de l'information

Les penseurs russes divisent la guerre de l'information selon deux domaines : information-psychologique et information-technique. Alors qu'en Occident l'approche au cyber s'est longtemps concentrée seulement sur ce qui se rapproche de l'aspect

[90] K. Giles (2016), *Handbook of Russian Information Warfare*, NATO Defense College, p.8, http://www.ndc.nato.int/news/news.php?icode=995
[91] *Ibid*, p.9.
[92] *Ibid*, p.10.
[93] *Ibid*, p.12.

information-technique (la sécurité des réseaux et des infrastructures critiques, les méthodes d'intrusion informatique, la guerre électronique, etc.), la Russie a, dès le milieu des années 1990, intégré l'aspect psychologique à l'aspect technique dans l'environnement informationnel. « The term information is being used in the description of Russia's Internet and military policies. Some Russian analysts have switched to the term cyber, but for the majority of the people writing on the topic, the focus remains on information. »[94]

L'aspect d'information-psychologique vise à protéger la société de l'influence informationnelle d'un adversaire. De même, des attaques d'information-psychologiques peuvent déstabiliser une société ennemie. Il s'agit d'un facteur de stabilisation et de déstabilisation de l'État. La stabilité est atteinte lorsque l'État contrôle les médias de masse et le flot d'informations. Il faut concevoir cette perspective dans le contexte de la désintégration de l'Union des républiques Socialistes Soviétique (U.R.S.S.), dont plusieurs analystes russes considèrent qu'il s'agissait d'une opération de guerre psychologique occidentale.[95] Cette analyse s'apparente à celle de Nye lorsqu'il affirme que le *soft power* des idées américaines a grugé de l'intérieur l'idéologie communiste jusqu'à la chute de l'U.R.S.S.[96]

Une autre caractéristique propre à la doctrine russe est que la guerre de l'information se mène à la fois en temps de paix et en temps de guerre.[97] Selon Saifetdinov, général russe retraité, « information warfare needs to be continuously conducted in peacetime, in periods of escalating threats, and in wartime. »[98] Il précise qu'en temps de

---

[94] T. Thomas (2014), *Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?,* The Journal of Slavic Military Studies, 27(1), p.101-102, https://www.tandfonline.com/doi/pdf/10.1080/13518046.2014.874845?needAccess=true

[95] R. Heickerö (2010), *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, Swedish Defence Research Agency (FOI), p.17-18, http://www.highseclabs.com/data/foir2970.pdf

[96] J. S. Nye (2009), *Get Smart: Combining Hard and Soft Power*, Foreign Affairs, 88(4), paragraphe: SUCCESS IN THE INFORMATION AGE, https://www.foreignaffairs.com/articles/2009-07-01/get-smart

[97] R. Heickerö (2010), *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, Swedish Defence Research Agency (FOI), p.18, http://www.highseclabs.com/data/foir2970.pdf
T. Thomas (1998), *Dialectical versus empirical thinking: Ten key elements of the Russian understanding of information operations*, The Journal of Slavic Military Studies, 11(1), p.44, https://www.tandfonline.com/doi/abs/10.1080/13518049808430328

[98] Citation de: Saifetdinov (2014), Informatsionnoe protivoborstvo v voennoi sfere [Information warfare in the military realm]. Voennaia mysl, (7), p.39, dans U. Franke (2015), *War by non-military means*

paix, la guerre de l'information doit se subordonner aux objectifs politiques. Dans cette situation, une proche collaboration entre les organisations militaires et civiles possédant les capacités appropriées est nécessaire. En temps de guerre, l'aspect crucial est de protéger les capacités de commandement et de contrôle permises par les moyens de communications modernes (de même que nuire à celles de l'adversaire).[99] Ainsi, « most theorists perceive information warfare as continuous between peace and war. The implication is clear: we are at the receiving end of Russian information warfare at this very moment. »[100]

c. Modélisation de la guerre de l'information (GI)

En reconnaissant l'absence de définition communément acceptée, Johnson pose comme point de départ de comprendre la GI comme :

> a form of comprehensive warfare, not merely a set of techniques. IW [Information Warfare] is differentiated from individual measures in that IW (like any other form of warfare) is governed by a strategy, which is focused on an objective. The strategy is a comprehensive plan for the use of IW-related weapons and tactics to attain the desired objective. The weapons and tactics may be any combination of military and nonmilitary techniques; the objective may be military, political, economic, or some combination thereof.[101]

Une modélisation fonctionnelle de la GI, selon Johnson, doit comporter trois éléments :

1. La description des objectifs et de la cible ultime.
2. L'identification et la liste des éléments techniques applicables à la GI.
3. La façon dont ces éléments se combinent dans une stratégie pour attaquer une cible.[102]

Son modèle définit trois niveaux de cibles : les systèmes d'information, la gestion de l'information et le processus de décision. L'attaque peut donc cibler la structure

---

Understanding Russian information warfare, Swedish Defence Research Agency (FOI), p.25, http://johnhelmer.net/wp-content/uploads/2015/09/Sweden-FOI-Mar-2015-War-by-non-military-means.pdf

[99] *Ibid*, p.26.

[100] *Ibid*, p.42.

[101] L. S. Johnson (2007), *Toward a Functional Model of Information Warfare*, CIA Library, paragraphe: A Starting Point, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/warfare.html

[102] *Ibid*, paragraphe: IW's Ultimate Target.

technique qui sous-tend le partage d'information, ou la capacité de transférer, disséminer, stocker, fusionner ou convertir cette information ou bien la façon dont l'information est utilisée. La cible ultime de la guerre de l'information est de façonner les perceptions, les décisions, les opinions ou les comportements de l'adversaire.[103]

Les moyens pour mettre en œuvre la GI sont doubles. Les moyens primaires de capacités techniques d'attaques et de défense sont à la base. Il peut s'agit de virus informatiques, d'opérations psychologiques (offensives) ou de méthodes d'encryptions (défensives). Il y a aussi des moyens de soutien. Il faut pouvoir collecter le renseignement de ciblage, évaluer l'impact des actions et détecter les attaques adverses par des indicateurs et des avertissements. [104] Il faut donc posséder des moyens d'actions, des capacités d'identification des vulnérabilités adverses, comprendre les effets sur la cible et se prémunir des attaques adverses à la fois par des capacités défensives et des moyens de détection.

La stratégie se définit en combinant les éléments à disposition pour l'attaque, la défense et le soutien avec les trois niveaux de cibles[105]. Il faut alors évaluer comment chaque élément peut affecter le système à chacun des trois niveaux pour comprendre la procédure employée lors de l'opération. Ce modèle sert donc de support à l'analyse d'une opération ou de la doctrine d'un acteur.[106] Il ne s'agit pas d'une description rigide. La difficulté est d'appliquer une compréhension des capacités d'un acteur avec les cibles visées pour définir la stratégie d'orchestration de l'opération.[107]

Johnson propose un modèle structurel des actes stratégiques dans une guerre de l'information. Sa description des objectifs est intéressante, mais bénéficierait de plus de précisions. Sa liste des techniques est nécessairement incomplète dans la mesure où elle date de 2007 et que celles-ci sont en constante évolution. De plus la compréhension stratégique des opérations est laissée à la discrétion de l'analyste, qui doit appliquer le

[103] *Ibid*, paragraphe: A Target Model.
[104] *Ibid*, paragraphe: The Elements of IW.
[105] Ces trois niveaux sont : les systèmes d'information, la gestion de l'information et le processus de décision.
[106] L'article de Johnson présente en exemple un tableau de son modèle au paragraphe : IW Orchestration.
[107] *Ibid*, paragraphe: IW Orchestration.

modèle aux divers actes de cette guerre. D'une façon semblable à ce modèle, les autres auteurs explorent aussi le sujet sous ces trois angles. Ils visent à répondre aux questions :

A. Quels sont les objectifs de ces opérations d'information?
B. Quelles techniques sont utilisées?
C. Comment ces techniques sont-elles déployées (c'est-à-dire quelle est la stratégie)?

Le modèle de Johnson servira donc de guide pour classifier les analyses effectuées sur l'approche russe à la guerre de l'information. Ce modèle pourrait certainement faire l'objet de bons nombres de critiques. En premier lieu, sa nature rationaliste implique une image du fonctionnement centralement organisé en fonction d'un objectif commun. Il ne rend pas compte du chaos de la lutte entre divers organismes bureaucratique dans le déploiement d'une action coordonnée. Ce modèle fait apparaître ces opérations comme étant mieux organisées et mieux coordonnées qu'elles ne le sont probablement en réalité. Ce modèle a cependant le grand avantage de fournir une vision large, englobante et complète des opérations d'information, ce qui est la perspective qui nous intéresse dans ce mémoire. En effet, plutôt que de se concentrer sur les luttes internes, humaines et organisationnelles, qui rendent la vie bureaucratique et étatique souvent sous-optimale et organisée moins rationnellement qu'il n'y paraît, le point focal est ici le fonctionnement d'ensemble qui est, somme toute, globalement rationnel en ce que les organisations font usage des moyens généralement appropriés pour atteindre leurs fins.

A. Objectifs de la Russie dans la guerre de l'information

Le renseignement américain a évalué que les objectifs russes durant les élections américaine de 2016 étaient de diminuer la confiance du public envers les institutions démocratiques et de favoriser l'élection d'un candidat au détriment d'un autre.[108] De plus,

[108] Office of the Director of National Intelligence – DNI (2017), *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, United States Government, p.ii, https://www.dni.gov/files/documents/ICA_2017_01.pdf

le Sénat américain affirme qu'une des priorités de Poutine est d'attaquer la démocratie américaine et de saper l'alliance transatlantique entre les États-Unis et l'Europe.[109]

Heickerö rapporte qu'une définition des objectifs de la guerre de l'information par des théoriciens militaires près du commandement russe est de « disorganize (disrupt) the functioning of the key enemy military, industrial and administrative facilities and systems, as well as to bring information-psychological pressure to bear on the adversary's military-political leadership, troops and population, something to be achieved primarily through the use of state-of-the-art information technologies and assets. »[110]

Cette pression contre le leadership politico-militaire et la population doit être comprise dans le contexte d'un retournement de la population contre ses dirigeants. Selon Franke, « this particular scenario – where the population turns against the political leadership – is a recurring theme in the Russian view of information warfare, clearly inspired by recent events such as the "colour" revolutions in former Soviet republics and the Arab spring. »[111]

Pour des auteurs comme Polyakova et Boyer, l'objectif de la Russie est encore de « divide, destabilize, and deceive democratic societies. »[112] Ce qu'indique Franke cependant est que cette division et cette déstabilisation visent à retourner la population contre ses élites dirigeantes. Pour l'école de pensée géopolitique d'Igor Panarin, « the so-called 'colour' revolutions in the CIS area and the 'Arab Spring' were a product of social control technology and information aggression from the United States. »[113] Selon Panarin, l'empire britanno-américain est sur le point de s'effondrer et son avantage dans la guerre

---

[109] U.S. Senate Committee on Foreign Relations (2018), *PUTIN'S ASYMMETRIC ASSAULT ON DEMOCRACY IN RUSSIA AND EUROPE: IMPLICATIONS FOR U.S. NATIONAL SECURITY*, United States Senate, p.1, https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

[110] R. Heickerö (2010), *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, Swedish Defence Research Agency (FOI), p.17, http://www.highseclabs.com/data/foir2970.pdf

[111] U. Franke (2015), *War by non-military means Understanding Russian information warfare*, Swedish Defence Research Agency (FOI), p.13, http://johnhelmer.net/wp-content/uploads/2015/09/Sweden-FOI-Mar-2015-War-by-non-military-means.pdf

[112] A. Polyakova et S. Boyer (2018), *The future of political warfare: Russia, the West, and the coming age of global digital competititon*, BROOKINGS – ROBERT BOSCH FOUNDATION TRANSATLANTIC INITIATIVE, p.3, https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf

[113] J. Darczewska (2014), *The anatomy of Russian information warfare*, Centre for Eastern Studies (OSW), p.15, http://aei.pitt.edu/57173/1/42.pdf

de l'information disparait.[114] Le courant de pensée parallèle est celui de l'école de Dugin. Elle considère que le libéralisme est la seule idéologie prédominante des pays occidentaux. De son côté, la Russie est une force révolutionnaire appelée à instaurer une idéologie post-libérale. « In its war on liberalism Russia will defend tradition, conservative values and true liberty. »[115]

Il faut donc concevoir que l'objectif spécifique de diviser et déstabiliser les pays de l'alliance transatlantique s'inscrit dans un but ultime plus vaste, celui de remplacer l'idéologie occidentale dominant l'ordre mondial depuis les années 1990, le libéralisme, par une idéologie russe des traditions, du conservatisme et d'une forme différente de ''liberté''.

Lamoreaux précise que l'agenda américain en Europe depuis les 80 dernières années a été de promouvoir et de protéger un ordre international libéral. Toutefois, propager cet ordre en Europe de l'Est et en Europe a été un défi complexe dans la mesure où il s'oppose à l'agenda russe dans la région.[116]

> The sources of friction between Russian and liberalist perspectives are that neither views the other as compatible. If the international liberal order is to succeed, states ought to be allowed to participate to the extent they wish. Russia's dominance of a specific region prevents this. However, if powers are to be balanced, one powers ideologies (and, thus, influence) should be considerably limited. Consequently, the US sees Russia preventing the spread of international liberalism, and Russia sees the US as interfering outside of its rightful sphere of influence.[117]

La guerre de l'information sert ainsi de soutien à l'atteinte des objectifs de politique étrangère du Kremlin. Il est nécessaire de placer les objectifs particuliers des opérations d'information dans le contexte plus large du conflit idéologique entre le libéralisme occidental et une idéologie conservatrice russe servant à maintenir l'emprise de Moscou sur sa sphère d'influence. Il n'en demeure pas moins que:

> The main goals of Russian information and influence operations include exploiting divisions in targeted states to achieve Russian foreign policy aims,

---

[114] *Ibid*, p.17.
[115] Citation de: A. Dugin (2009), The Fourth Political Theory, dans *Ibid*, p.19.
[116] J. W. Lamoreaux (2019), «The Three Motivations for an Assertive Russian Grand Strategy », dans N. Peterson (dir.) *Russian Strategic Intentions*, NSI, Inc., rapport pour le Département de la défense des États-Unis, p.1, https://nsiteam.com/sma-white-paper-russian-strategic-intentions/
[117] *Ibid*, p.5.

> ensuring continued domestic support for the regime, maintaining compliant governments in other states, keeping unfriendly governments weak and off balance, and influencing international perceptions of Russian actions while excluding Western sway from Moscow's sphere of influence.[118]

Les opérations d'information menées par Poutine visent ainsi à saper les fondements même de la démocratie. La diminution de la confiance et le discrédit envers les processus électoraux, médiatiques et politiques est plus importante pour Moscou que l'élection d'un candidat particulier. La perte de repaire des populations occidentales génère un chaos dont le régime du Kremlin peut profiter pour faire avancer ses intérêts à l'étranger et solidifier sa position intérieure.[119]

B. Techniques des opérations d'information

De nombreux auteurs ont traité, analysé et classifié les techniques utilisées par la Russie pour étendre son influence dans la sphère informationnelle occidentale. Leurs classifications sont assez semblables et elles se distinguent essentiellement par le détail et la complétude de leur analyse, plutôt que par des désaccords de fonds.

Polyakova et Boyer identifient trois catégories d'outils d'influence : les campagnes de désinformation, les alliés politiques dans les démocraties occidentales et les cyberattaques.[120]

- La désinformation est disséminée à la fois ouvertement par les médias officiels russes et secrètement dans les médias sociaux par des ''trolls''[121], des ''bots''[122] et des faux comptes. Les méthodes employées sont :

---

[118] R. Weitz (2019), « Moscow's Gray Zone Toolkit », p.21-22, dans *Ibid.*, p.21-22.
[119] S. L. Hall (2017), *General Chaos is the Kremlin's Favorite Candidate*, Cipher Brief, https://www.thecipherbrief.com/general-chaos-kremlins-favorite-candidate?fbclid=IwAR29mpcZWUqj5X4mwNEMEayduuqyQvjLuQPHTELzKuJt0QfBWkkHLqdS8mw
[120] A. Polyakiva et S. Boyer (2018), *The future of political warfare: Russia, the West, and the coming age of global digital competititon*, BROOKINGS – ROBERT BOSCH FOUNDATION TRANSATLANTIC INITIATIVE, p.4-10, https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf
[121] Les ''trolls'' sont de utilisateurs des médias sociaux visant à susciter des polémiques.
[122] Un ''bot'' est un programme informatique permettant de répéter automatiquement une tâche, par exemple publié sur les réseaux sociaux, ou de simuler les comportements d'une personne.

1. La propagation et l'amplification d'informations trompeuses, fausses ou polarisantes.
2. Le déploiement d'une propagande automatisée permet une vaste diffusion rapide de contenus répétés.
3. L'accentuation des tensions et des vulnérabilités sociales.

- Moscou cultive des liens avec de nombreux partis et mouvements de gauche comme de droite. En Europe, certains partis politiques, comme le Front National, l'*Alternativ für Deutschland* ou la Ligue Italienne, ont des accords de coopération officiels avec le parti de Poutine, le *United Russia Party*.
    1. La Russie peut apporter du soutien financier, diplomatique et médiatique à ces partis.
- Des cyberattaques sont menées par des agences gouvernementales russes (GRU[123], FSB[124], FSV[125]), des pirates informatiques au service de ces agences (APT[126] 28 et 29, CyberBerkut) ou des associés informels (cyber criminels, firmes de hautes technologies et cyber activistes). De plus, ces actions sont parfois appuyées par des acteurs supposément indépendants, comme WikiLeaks. Ces groupes font :
    1. De l'hameçonnage (vols d'informations sensibles, tels que des mots de passes, par le moyen de courriels trompeurs)
    2. Des attaques de déni de service (surcharge de serveurs informatiques pour en empêcher l'accès par les utilisateurs légitimes)
    3. Ils utilisent des titres et informations officiels obtenus d'une cible précédente pour approcher une nouvelle cible.

[123] Renseignement militaire
[124] Renseignement civil extérieur
[125] Renseignement civil intérieur
[126] APT = Advanced Perceived Threat. L'expression APT provient de la *United States Air Force* et est maintenant utilisé par la majorité des agences de renseignement occidentales. Les noms virtuels de ces groupes varient. APT29 est aussi connu sous le nom de Cozy Bear, tandis que APT28 sous les noms de Tsar Team, Sofacy et Pawn Storm.

Ajir et Vailliant utilisent une classification semblable en parlant de l'exploitation des médias sociaux par des cybers capacités, du contrôle des médias occidentaux et du lobbying dans la société occidentale.[127]

- La Russie déploie plusieurs actions dans les médias sociaux et le cyberespace :
    1. Les *bots* et les *trolls* propagent extrêmement rapidement les discours de propagande.
    2. Ce discours est aussi disséminé par des comptes officiels tels que ceux des ambassades russes. La diplomatie publique est donc considérée comme une partie active des campagnes de désinformation.
    3. La collecte d'informations sur des individus.
    4. Les informations obtenues peuvent permettre de contraindre des acteurs opposés au Kremlin. Ils peuvent être menacés, intimidées ou voir leur réputation entachée par de vraies ou fausses révélations embarrassantes.
- Le contrôle des médias occidentaux passe par divers canaux :
    1. Des chaînes médiatiques russes comme *Russia Today* ou *Sputnik.*
    2. Par l'achat d'espace dans les grands médias occidentaux. La Russie veut se donner une image plus libérale en adaptant ce contenu à l'esprit ''critique'' des Occidentaux. Elle souhaite influencer l'opinion publique en partageant son point de vue sur les événements géopolitiques.
    3. Des acteurs fortunés et proches du pouvoir russe achètent des journaux occidentaux au bord de la faillite pour en faire des publications favorables au Kremlin.
- Les lobbys occidentaux et la société civile se présentent sous plusieurs formes :
    1. Les hommes d'affaires russes sont encouragés à financer des partis politiques et des politiciens occidentaux favorables à Moscou.
    2. La création et l'appui à des organisations non-gouvernementales (ONG) dont l'idéologie s'aligne sur celle du pouvoir russe. Ces organisations exportent cette

[127] M. Ajir et B. Vailliant (2018), *Russian Information Warfare : Implications for Deterrence Policy*, Strategic Studies Quarterly, 12(3), p.75-81, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Ajir.pdf

influence idéologique à travers des groupes de réflexion, des tables rondes, des conférences, etc.

3. L'embauche de firmes occidentales de relations publiques permet d'améliorer l'image du Kremlin à l'étranger. Ces firmes emploient souvent d'anciens politiciens, ambassadeurs ou hauts représentants du gouvernement qui ont un accès direct aux sphères du pouvoir. Ils effectuent ainsi du lobbyisme pour Moscou.

Laurinavicius reprend de façon générale les mêmes thèmes en parlant du financement public et secret à des acteurs occidentaux favorables au Kremlin, du soutien et des liens avec certains partis politiques ou organisations non-gouvernementales occidentales, à la collecte maligne d'information par des cyberattaques ou de l'espionnage traditionnel, des campagnes de désinformation dans les médias officiels et les médias sociaux.[128] Même chose chez Weitz, qui utilise les thèmes de la désinformation, du soutien aux groupes d'opposition de gauche et de droite et la promotion d'organisations culturelles (ONGs, l'église orthodoxe, etc.).[129]

L'organisme *EU vs Disinformation* identifie quatre catégories de méthodes d'influence électorale : la manipulation de l'information, les cybers perturbations, le soutien aux élites ou aux partis politiques et les interventions extrêmes. Les trois premières catégories correspondent à ce qui a été précédemment défini. Les interventions extrêmes rendent compte de l'intervention militaire directe lorsque l'influence indirecte échoue à obtenir les résultats désirés. Des opérations d'information sont conduites simultanément à ces interventions pour contrôler le message entourant le conflit. Cette catégorie réfère en particulier aux événements de Géorgie en 2008 et d'Ukraine en 2014.[130] Mölder et Sazonov expliquent que la guerre de l'information dans un contexte d'intervention militaire hybride

[128] M. Laurinavičius (2018), *A Guide to the Russian Tool Box of Election Meddling*, International Election Study Center (IESC), p.3, http://iesc.lt/app/uploads/2018/10/IESC_Guide_ToolBox_2018_FINAL.pdf
[129] R. Weitz (2019), « Moscow's Gray Zone Toolkit », dans N. Peterson (dir.) *Russian Strategic Intentions*, NSI, Inc., rapport pour le Département de la défense des États-Unis, p.22, https://nsiteam.com/sma-white-paper-russian-strategic-intentions/
[130] EU vs Disinformation (2019), *Methods of Foreign Electoral Interference*, European External Action Service East Stratcom Task Force, https://euvsdisinfo.eu/methods-of-foreign-electoral-interference/

fait, entre autres, usage de l'ensemble des canaux d'informations (médias, internet, téléphones, haut-parleurs) pour convaincre, désorienter, apeurer ou faire paniquer la population et les soldats.[131]

Trois larges catégories de techniques se dégagent donc de cette revue documentaire. Dans la guerre de l'information, la Russie :

1. Use de méthodes de propagande ou de désinformation à la fois dans les médias officiels et dans les réseaux sociaux.
2. Appuie, embauche et s'associe à des organisations politiques et non-gouvernementales partageant ses intérêts ou ses conceptions idéologiques.
3. Agit dans le cyberespace pour s'introduire dans des serveurs sécurisés, collecter de l'information, introduire des programmes malveillants ou diffuser des informations dommageables pour des individus ou des organisations.

Par ailleurs, ces méthodes s'appliquent à la fois en temps de paix et d'une façon similaire mais particulière durant les conflits hybrides.

C. La stratégie de déploiement opérationnel

> [The] essence of strategy is that IW [Information Warfare] is the purposeful training or persuasion of an enemy to get him to do something seemingly for himself but in actuality doing something that benefits you.[132]
>
> - Timothy Thomas

La question principale que pose cette recherche est: quelle stratégie la Russie utilise-t-elle pour persuader un adversaire de faire une action la bénéficiant au détriment

[131] H. Mölder et V. Sazonov (2018), *Information Warfare as the Hobbesian Concept of Modern Times — The Principles, Techniques, and Tools of Russian Information Operations in the Donbass*, The Journal of Slavic Military Studies, 31(3) p.322-325, https://www.tandfonline.com/doi/full/10.1080/13518046.2018.1487204

[132] T. Thomas (2014), *Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?*, The Journal of Slavic Military Studies, 27(1), p.104, https://www.tandfonline.com/doi/full/10.1080/13518046.2014.874845

de ses propres intérêts? Un processus sophistiqué d'exploitation de vulnérabilités sociales et technologiques semble en effet impliquer l'utilisation d'une stratégie réfléchie, planifiée et concrétisée.[133] Le concept indiquant le plus précisément cette idée est celui de contrôle réflexif (CR). « Reflexive control is the term used to describe the practice of predetermining an adversary's decision in your favor, by altering key factors in the adversary's perception of the world. »[134] Il s'agissait d'un concept utilisé à l'époque soviétique, mais qui est fréquemment revenu dans la documentation occidentale suite à la résurgence des opérations d'information russes. Deux définitions du contrôle réflexif apparaissent dans la documentation russophone :

- « The process of intentionally conveying to an opposing side of a certain aggregate information (attributes) which will cause that side to make a decision appropriate to that information. »[135]
- « Reflexive control consists of transmitting motives and grounds from the controlling entity to the controlled system that stimulate the desired decision. The goal of RC is to prompt the enemy to make a decision unfavorable to him. Naturally, one must have an idea about how he thinks. »[136]

Trois éléments se dégagent de ces définitions.

1. Le CR vise ultimement la prise de décision de la cible.
2. L'information transmise doit orienter vers une décision ou une prise de position.
3. L'information doit être adaptée à la logique, la culture, la psychologie et les émotions de la cible.

[133] *Ibid*, p.105.
[134] K. Giles, J. Sherr et A. Seaboyer (2018), *Russian Reflexive Control*, Royal Military College of Canada, Rapport pour Defence Research and Development Canada, p.4, http://cradpdf.drdc-rddc.gc.ca/PDFS/unc323/p807769_A1b.pdf
[135] Citation de: F. Chausov (1999), Osnovy Refleksivnogo Upravleniya Protivnikom, Morskoi Sbornik, No. 9, p. 12, dans *ibid*, p.5.
[136] Citation de: S. Leonenko (1995), Refleksivnoye Upravlenie Protivnikom, Armeyskiy Sbornik, No.8, pp.27-32, dans *ibid*, p.5.

Pour mener à bien ce processus, un penseur russe de la guerre de l'information, Sergey Komov, a défini une série de mesures pouvant induire une prise de décision défavorable à la cible[137] :

- Distraction : en créant un adversaire imaginaire dans un emplacement vital qui force la cible à reconsidérer sa présente action.
- Surcharge : en envoyant fréquemment une grande quantité d'informations.
- Paralysie : en créant une perception de menace à un intérêt vital ou un point faible.
- Fatigue : en incitant l'adversaire à mener des opérations inutiles.
- Tromperie : en forçant l'adversaire à réallouer des ressources dans un endroit supposément menacé.
- Division : en convaincant l'adversaire qu'il doit agir en opposition aux intérêts de sa coalition.
- Pacification : en menant l'adversaire à croire que les actions prises ne sont que des entraînements et non des opérations offensives.
- Dissuasion : en créant la perception d'une supériorité insurmontable.
- Provocation : en incitant l'adversaire à effectuer une action désavantageuse pour son camp.
- Suggestion : en offrant des informations influençant l'adversaire légalement, moralement ou idéologiquement.
- Pression : en offrant des informations qui discrédite le gouvernement aux yeux de la population.

Ces mesures peuvent être appliquées individuellement ou conjointement. Elles ne mènent pas nécessairement à une prise de décision immédiate, mais peuvent aussi créer un environnement défavorable qui conduit à une série de décisions sous-optimales.

Une stratégie de contrôle réflexif doit donc commencer par déterminer la décision ou la direction qu'il est souhaitable que la cible prenne. Par la suite, une démarche

[137] Citation de: S. A. Komov (1997), About Methods and Forms of Conducting Information Warfare, Military Thought, No. 4, pp. 18–22, dans *Ibid*, p.6.

stratégique peut être établie faisant usage des mesures appropriées pour conduire aux conséquences voulues.

La cible peut être un individu tout comme un collectif. Les individus ciblés sont ceux dont la décision aura un fort impact sur les actions (président, premier ministre, ministre, général, etc.). Les collectifs sont visés pour l'impact qu'ils peuvent avoir sur les individus prenant des décisions critiques. Les collectifs peuvent paralyser ou suggérer des actions, induire une fatigue, inciter à la division, etc. Une analyse précise de la cible est aussi une étape importante afin d'adapter le contenu de l'information présentée aux schèmes cognitifs de la cible. Ceci permet de prédire les réactions de la cible aux informations présentées.[138]

Le CR se déploie généralement sur le long terme. La capacité de modifier les perceptions et éventuellement la prise de décision d'une cible est complexe et dépend de nombreux facteurs. Ces opérations peuvent impliquer des programmes en apparence distincts, mais dont les impacts cumulatifs selon des vecteurs différents mènent au résultat escompté à long terme.[139]

Comme il a été présenté précédemment, un processus de CR fait notamment usage de propagande ou de désinformation pour influencer la cible. Paul et Matthews caractérisent la propagande russe par son haut volume, l'usage de multiples canaux de communications, sa rapidité, sa continuité, sa répétitivité, son inconsistance et son utilisation fréquente de demi-vérités et de faussetés.[140] Ces caractéristiques sont conformes aux mesures de Komov.

d. Stratégies de contrôle réflexif

Une compréhension fine du processus stratégique ne peut se faire qu'avec l'étude des cas particuliers où il a été déployé. En effet, l'importance pour le CR d'être adapté à sa

[138] *Ibid*, p.7-8
[139] *Ibid*, p.53.
[140] C. Paul et M. Matthews (2016), *The Russian ''Firehose of Falsehood'' Propaganda Model*, Rand Corporation, p.2-8, https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf

cible implique une singularité propre à chaque opération. Par contre, les objectifs communs poursuivis nécessitent qu'un processus similaire soit employé dans ces opérations, ne serait-ce que pour conserver la cible dans la direction voulue. Par ailleurs, la variété d'acteurs et d'organisations impliqués impose la mise en place d'une forme de coordination pour que tous agissent selon des lignes directrices communes. Dans les mots du théoricien russe Vorobev, « since there are a lot of forces of different kinds involved when conducting information warfare, an organization for precise coordination is required »[141]. Cette coordination, c'est-à-dire le déploiement stratégique des opérations, a peu fait l'objet d'études de la part des chercheurs en sources ouvertes. C'est cette problématique que la présente étude tente d'éclaircir.

[141] Citation de : Vorobev (2007), Informatsionno-udarnaia operatsiia [The information shock operation], Voennaia mysl, Vol.6, p.14–21, dans U. Franke (2015), *War by non-military means Understanding Russian information warfare*, Swedish Defence Research Agency (FOI), p.24, http://johnhelmer.net/wp-content/uploads/2015/09/Sweden-FOI-Mar-2015-War-by-non-military-means.pdf

VI. Étude de cas – Les opérations d'information russes en occident de 2007 à 2017

A. Le choc pour les pays baltes de la cyberattaque de 2007 en Estonie

> These attacks (…) represent a new kind of war where the threat lies not in conventional armies but in a wholly asymmetric or unconventional attack deploying one or another form of IW. (…) In such a war, of course, it is not the enemy army that is targeted, but rather the entire society and political structure become targets. (…) What we see here is merely the latest crystallization of this new but previously foretold kind of war.[142]
>
> - Stephen Blank, 2008

a. Cyberattaque, diplomatie publique et manifestations populaires

La première guerre de l'information moderne d'Europe est liée aux événements d'avril et de mai 2007 en Estonie. Le 27 avril, le gouvernement estonien déplaçait dans la ville de Tallinn une statue nommée *Le Soldat de bronze*, qui symbolisait, pour les Soviétiques et maintenant les Russes, la libération de l'Estonie durant la Seconde Guerre mondiale. Suite à cet événement controversé, les infrastructures de télécommunication d'Estonie, les sites de divers ministères, deux banques et plusieurs partis politiques ont subi des cyberattaques d'envergures durant des semaines.[143] Ces attaques étaient principalement constituées des dénis de service (DDoS) et de ''botnets''[144]. Moscou est désigné par le gouvernement estonien et plusieurs analystes comme étant à l'origine de ces attaques.[145] La première phase de l'attaque (du 27 au 29 avril) était simple et démontrait un faible niveau de coordination. Elle a débuté suite à la publication sur divers forums internet russes

---

[142] S. Blank (2008), *Web War I: Is Europe's First Information War a New Kind of War?,* Comparative Strategy, 27(3), p.227, https://www.tandfonline.com/doi/pdf/10.1080/01495930802185312?needAccess=true

[143] S. Herzog (2011), *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, Journal of Strategic Security, 4(2), p.51, https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss

[144] « Botnet est un terme générique qui désigne un groupe d'ordinateurs infectés et contrôlés par un pirate à distance. » - D. Fischer (2013), *Qu'est-ce qu'un botnet?*, Kapersky daily, https://www.kaspersky.fr/blog/quest-ce-quun-botnet/888/

[145] S. Blank (2008), *Web War I: Is Europe's First Information War a New Kind of War?,* Comparative Strategy, 27(3), p.227, https://www.tandfonline.com/doi/pdf/10.1080/01495930802185312?needAccess=true

des instructions de commandes *ping* qui permettent d'initier des attaques DDoS.[146] Une explication possible est que des agents de l'État aient distribué les codes d'opérations de ces attaques, qui ont pu par la suite être reprises par tout pirate informatique qui souhaitait amplifier l'opération. L'intensité et la coordination des attaques ont par la suite augmentées lors d'une seconde phase entre le 30 avril et 18 mai.[147]

Le Kremlin a aussi publiquement menacé l'Estonie de rompre ses liens diplomatiques, alors que des députés ont traité le gouvernement estonien de fasciste et déclaré que le retrait de la statue était un acte barbare et blasphématoire.[148] Durant la même période, des manifestations violentes ont été organisées à Tallinn parmi la diaspora russe d'Estonie. Une enquête des autorités estoniennes a révélé que ces manifestations avaient commencées à être planifiées un an avant le début des événements.[149] D'autres manifestations ont eu lieu contre l'ambassade estonienne à Moscou. Les manifestations en Russie provenaient de l'organisation pour la jeunesse russe *Nachi*, un groupe nationaliste créée par le régime de Vladimir Poutine.[150]

Selon Blank, ces opérations entreprises contre l'Estonie reflétaient une stratégie coordonnée, sanctionnée par de hautes instances politiques, et planifiée bien avant le retrait du *Soldat de bronze*.[151]

b. Propagande médiatique et désinformation

En 2005, le lancement de la *Baltic Media Alliance* créait la principale source de propagande télévisuelle russe dans les pays baltes.[152] Ce groupement médiatique diffuse dans les trois pays baltes, alors que la télévision reste la principale source d'information

[146] A. Randin (2017), *Hybrid Warfare in the Baltics*, RAND Corporation, p.19.
[147] *Ibid*, p.19.
[148] L. Harding (2007), *Russia up in arms after Estonians remove statue of Soviet soldier*, The Guardian, https://www.theguardian.com/world/2007/apr/28/russia.lukeharding
[149] S. Blank (2008), *Web War I: Is Europe's First Information War a New Kind of War?,* Comparative Strategy, 27(3), p.228.
[150] *Ibid*, p.228.
[151] *Ibid*, p.228.
[152] A. Krol (2017), *Russian Information Warfare in the Baltic States — Resources and Aims*, Warsaw Institute, paragraphe: Control the Media, Rule the World, https://warsawinstitute.org/russian-information-warfare-baltic-states-resources-aims/

des populations de la région. Plusieurs plateformes numériques, dont les principales sont *Sputnik* et *Baltnews*, servent de diffuseur web pour le point de vue du Kremlin. Ces plateformes intègrent à la fois actualité et divertissement. Elles se décrivent souvent comme présentant une vision alternative des événements. Par ailleurs, les productions audiovisuelles provenant de Russie sont d'une qualité supérieure aux productions locales. L'auditoire cible est la population russophone disséminée en Estonie, en Lettonie et en Lituanie. Les minorités russophones comptaient en 2011 pour environ 35% de la population en Lettonie, 30% en Estonie et 8% en Lituanie. Ce groupe ethnolinguistique vit donc dans une sphère informationnelle distincte par rapport au reste de la population.[153]

La désinformation russe vise à provoquer, justifier ou renforcer un sentiment d'injustice et d'insécurité dans cette diaspora. Une étude de 2008 concluait que seulement 12% des Russes vivant en Lituanie se sentait discriminé, mais qu'en Lettonie se sentiment augmentait à 25% de cette population, tandis qu'en Estonie il était à 55%.[154] Les thèmes de cette désinformation se regroupent autour de la réémergence du fascisme, de la russophobie, du nettoyage ethnique des populations russophones et des comportements inappropriés des soldats de l'OTAN (Organisation du Traité de l'Atlantique Nord).[155]

Des groupes d'activistes et des organisations non-gouvernementales pour les droits des Russophones représentent une avenue supplémentaire de redistribution de cette information. Des fonds provenant de Russie, tel que le « Fond pour le Soutien et la Défense des Compatriotes à l'étranger » servent à financer et soutenir ces organisations.[156] En se faisant l'écho des inquiétudes et préoccupations des minorités russophones dans les pays

---

[153] A. Randin (2017), *Hybrid Warfare in the Baltics*, RAND Corporation, p.14-18. https://www.rand.org/pubs/research_reports/RR1577.html#download

[154] M. Best (2013), *The Ethnic Russian Minority: A Problematic Issue in the Baltic States*, Verges: Germanic and Slavic Studies in review, 2(1), p.38, https://journals.uvic.ca/index.php/verges/article/view/11634

[155] A. Krol (2017), *Russian Information Warfare in the Baltic States — Resources and Aims*, Warsaw Institute, paragraphe: Narratives most widespread in the media, https://warsawinstitute.org/russian-information-warfare-baltic-states-resources-aims/
EU vs Disinformation (2018), *Baltic Brutality?*, European External Action Service East Stratcom Task Force, https://euvsdisinfo.eu/baltic-brutality/

[156] C. M. Collier (2016), *Latvia in the Crosshairs: Russian Information Warfare and Appropriate Countermeasures*, Small Wars Journal, https://smallwarsjournal.com/jrnl/art/latvia-in-the-crosshairs-russian-information-warfare-and-appropriate-countermeasures#_edn9

baltes, ils diffusent aussi la propagande et la désinformation russe visant à nourrir ces inquiétudes.

Ce contrôle de l'environnement informationnel d'une partie de la population a un impact réel sur l'opinion de celle-ci par rapport à des sujets clés pour Moscou. Ainsi, une étude longitudinale entre les années 2000 et 2014 de l'attitude envers l'OTAN des populations estoniennes et non-estoniennes (c'est-à-dire les populations russophones) a montré que la variation de cette opinion peut être liée à la couverture des événements internationaux par les médias de langue russe. Ce sondage démontre que les populations estoniennes avaient en 2014 une attitude favorable à 97% envers l'OTAN, comparativement à seulement 44% chez les populations russophones. De plus, cet appui de 44% était en déclin par rapport à l'année 2013, alors qu'il était de 52%. Du côté de la population estonienne, l'appui de 97% était plutôt en augmentation par rapport aux 88% en 2013.[157] Cette variation opposée est en corrélation avec la crise ukrainienne, dont l'interprétation qu'en ont propagée les médias russes était bien différente de celle de leurs vis-à-vis occidentaux.

Plus récemment, les discours du président Poutine sur la protection des populations russophones hors de la Russie ciblent, entre autres, cette diaspora en Estonie. Ce discours a notamment servi à justifier la saisie de territoires en Ukraine. Cela fait donc augmenter les craintes des autorités des pays baltes que le Kremlin tente une opération semblable dans leur région. Pour cette raison, la propagande médiatique, source de discorde entre ces groupes ethnolinguistiques et pouvant servir de prétexte à une intervention militaire, est préoccupante.[158]

---

[157] J. Kivirähk (2014), *Integrating Estonia's Russian-Speaking Population: Findings of National Defense Opinion Surveys*, International Centre for Defence and Security: Estonia, p.15-17, https://icds.ee/wp-content/uploads/2014/Juhan_Kivirahk_-_Integrating_Estonias_Russian-Speaking_Population.pdf

[158] C. S. Chivvis (2017), *Understanding Russian "Hybrid Warfare" and What Can be Done About It*, RAND Corporation, Testimony presented before the House Armed Services Committee, p.3, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

B. La guerre russo-géorgienne de 2008

> Cyberattacks in the Russia-Georgia War Reaffirm the Russian View of Cyberspace as a Tool for Psychological Manipulation and Information Warfare.[159]
>
> - Sarah P. White

a. Contexte

Le statut de territoire autonome de l'Ossétie du Sud a constitué la trame de fond de la guerre russo-géorgienne. Alors que ce territoire réclame son indépendance et que la Russie est intervenue à ses côtés, la Géorgie a plutôt tenté de réintégrer militairement celui-ci par une offensive terrestre. Durant ces événements, une opération d'information s'est déroulée parallèlement et en soutien à une opération militaire conventionnelle. C'était la première guerre durant laquelle les éléments de terre, de mer, d'air et du cyberespace étaient utilisés de façon synchronisée.[160] La Géorgie, tout comme la Russie, a mené des activités de contrôle de l'information afin de favoriser son interprétation de la situation aux yeux des populations et de la communauté internationale.[161] Toutefois seules les actions russes seront ici exposées.

b. Cyberattaques

Trois semaines avant le début du conflit militaire, la Géorgie était victime d'attaques de dénis de service (DDoS) et de dégradation de sites internet[162]. Des sites liés aux communications, à la finance et au gouvernement ont été affectés.[163] Un site populaire

---

[159] S. P. White (2018), *Understanding Cyberwarfare Lessons from the Russia-Georgia War*, Modern War Institute at West Point, p.2, https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf

[160] D. Hollis (2011), *Cyberwar Case Study: Georgia 2008*, Small Wars Journal, p.2, https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

[161] E. J. Iasiello (2017), *Russia's Improved Information Operations: From Georgia to Crimea*, Parameters, 47(2), p.52, https://publications.armywarcollege.edu/pubs/3368.pdf

[162] Traduction libre pour: website defacement. Il s'agit d'une pratique consistant à remplacer la page ciblée par une image ou un message de propagande, insultant, pornographique, dégradant ou autre.

[163] D. Hollis (2011), *Cyberwar Case Study: Georgia 2008*, Small Wars Journal, p.2, https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

de Géorgie pour les pirates informatiques a aussi été visé avec l'objectif de mitiger une éventuelle contre-attaque de la part des pirates géorgiens.[164] Ces attaques se sont poursuivies durant les cinq journées qu'ont duré les affrontements militaires. Cela a causé de la confusion et a nui à la capacité du gouvernement géorgien de communiquer efficacement avec la population. En limitant la capacité du gouvernement de réagir rapidement, durant les premiers jours du conflit, pour communiquer son message à la communauté internationale, cela a donné le temps nécessaire à la Russie pour définir la première interprétation de cette crise.[165]

Il existe trois possibilités quant à l'origine de ces attaques : soit le gouvernement russe les a exécutées lui-même, soit il a diffusé sur internet des méthodes et des cibles pour que des pirates informatiques patriotiques les exécutent, soit elles ont été spontanément effectuées par des communautés de citoyens, des groupes criminels et des pirates informatiques indépendants.[166] Bien que les preuves disponibles ne permettent pas de conclure avec certitude que le gouvernement russe ait été derrière ces attaques, il est certain que celui-ci en a bénéficié.[167]

Il serait toutefois surprenant que le gouvernement n'ait pas été impliqué dans la planification de ces attaques considérant l'étroite coordination entre les objectifs stratégiques du gouvernement et les opérations dans le cyberespace. Par exemple, les infrastructures critiques comme les réseaux gaziers et pétroliers ou les centrales électriques n'ont pas été visées par des cyberattaques. Celles-ci auraient causé une véritable panique et un chaos dans la population. Cette instabilité civile aurait pu être un prétexte d'intervention militaire occidentale, ce que Moscou voulait éviter. De la même façon, les bombardements de l'aviation russe n'ont pas ciblé le pipeline Baku-Ceyhan, bien qu'ils aient bombardés partout autour. Ce pipeline était une raison majeure pour laquelle les pays de l'Ouest se préoccupaient du conflit et sa destruction aurait aussi constitué un prétexte

---

[164] *Ibid*, p.3.
[165] S. P. White (2018), *Understanding Cyberwarfare Lessons from the Russia-Georgia War*, Modern War Institute at West Point, p.1-2 https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf
[166] R. J. Deibert, R. Rohozinski et M. Crete-Nishihata (2012), *Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war*, Security Dialogue, 43(1), p.17, https://journals.sagepub.com/doi/pdf/10.1177/0967010611431079
[167] *Ibid*, p.12-17.

d'intervention armée.[168] Ce type de coordination entre les objectifs stratégiques du gouvernement et les actions des pirates informatiques semblent étayer un rôle actif de Moscou dans la synchronisation de celles-ci.[169]

c. Propagande médiatique

Les médias russes ont défendu la perspective selon laquelle la Russie effectuait une mission d'imposition de la paix en Géorgie. L'armée russe serait ainsi intervenue en Géorgie pour venger la mort d'une cinquantaine de membres de leur force de maintien de la paix[170] et défendre l'autonomie de l'Ossétie du sud contre l'invasion géorgienne.[171] Toutefois, cette posture conceptuelle est exagérée considérant que leur intervention militaire dénommée « mission d'imposition de la paix » n'avait pas l'aval de l'Organisation des Nations Unies (ONU).[172] Pour son intervention militaire, la Russie a appliqué les leçons apprises des principes de légitimation propre aux pays de l'Ouest. Elle a ainsi considéré qu'il était légitime d'intervenir pour protéger des minorités opprimées, effectuer une intervention humanitaire et faire une attaque préemptive contre une force qui pourrait la cibler.[173] C'est ainsi que les justifications officielles du président Medvedev étaient que l'armée russe intervenait en réponse à une violation du droit international, pour prévenir une catastrophe humanitaire, protéger la vie et la dignité de citoyens russes et punir les responsables de ces crimes.[174]

---

[168] D. Hollis (2011), *Cyberwar Case Study: Georgia 2008*, Small Wars Journal, p.4, https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf
[169] *Ibid*, p.5.
[170] L'armée russe avait des troupes dans la « Joint control Commission for Georgian-Ossetian Conflict Resolution » qui déployait une force de maintien de la paix en Ossétie du Sud depuis 1992.
[171] T. Thomas (2009), *The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia*, Slavic Military Studies, 22(1), p.32-34. https://www.tandfonline.com/doi/pdf/10.1080/13518040802695241?needAccess=true
[172] *Ibid*, p.34-35.
[173] *Ibid*, p.40.
[174] H.-G.Heinrich et K. Tanaev (2009), *Georgia & Russia : Contradictory Media Coverage of the August War,* Caucasian Review of International Affairs, 3(3), p.248, http://www.cria-online.org/Journal/8/Done_Georgia-Russia_Contradictory%20Media%20Coverage%20of%20the%20August%20War_Heinrich_Tanaev.pdf

Les médias russes ont aussi utilisé cette ligne argumentaire pour comparer cette opération militaire à des interventions passées de l'OTAN, en particulier celle au Kosovo.[175] C'était à la fois une façon de justifier leur position face à la communauté internationale et de discréditer celle de l'OTAN face aux critiques occidentales. Des entrevues quotidiennes avec des porte-paroles militaires et des reportages télévisés montraient le progrès des troupes protégeant les citoyens russes. Cela était mis en opposition aux atrocités commises par les troupes géorgiennes. Cette campagne a été partiellement efficace, alors qu'à un moment du conflit, un sondage de CNN indiquait que 92% des répondants croyaient que l'intervention militaire russe était justifiée.[176]

d. Opération psychologique

Dans une perspective stratégique globale, l'ensemble de la guerre russo-géorgienne peut être considérée comme une opération de guerre psychologique (PSYOP). En effet, le président de Géorgie, Mikhail Saakashvili, a été incité par la Russie à déclencher cet affrontement militaire désavantageux.[177] La Secrétaire d'État de l'époque, Condoleezza Rice, avait averti le président Saakashvili de ne pas tomber dans le piège des provocations russes. Elle disait de lui: « He's proud and can be impulsive, and we all worried that he might allow Moscow to provoke him to use force. »[178] Il est donc possible, comme le pense Madame Rice, que les bombardements par les séparatistes d'Ossétie du Sud sur des villages à la frontière de la Géorgie avaient comme but de provoquer l'offensive géorgienne. Cette hypothèse est renforcée par l'état de préparation élevé et la réaction rapide des forces russes, qui indique une planification antérieure avancée.[179]

---

[175] E. J. Iasiello (2017), *Russia's Improved Information Operations: From Georgia to Crimea*, Parameters, 47(2), p.53, https://publications.armywarcollege.edu/pubs/3368.pdf
[176] *Ibid*, p.53.
[177] D. Baker, K. Fermaint et M. D. Neff (2013), *The Russia-Georgia War of 2008: Information Operations Case Study Analysis*, p.19, https://www.academia.edu/11903525/The_Russia-Georgia_War_of_2008_Information_Operations_Case_Study_Analysis
[178] J. Kucera (2011), *Condoleezza Rice Warned Georgian Leader on War With Russia*, The Atlantic, https://www.theatlantic.com/international/archive/2011/11/condoleezza-rice-warned-georgian-leader-on-war-with-russia/248560/
[179] D. Baker, K. Fermaint et M. D. Neff (2013), *The Russia-Georgia War of 2008: Information Operations Case Study Analysis*, p.20, https://www.academia.edu/11903525/The_Russia-Georgia_War_of_2008_Information_Operations_Case_Study_Analysis

En accusant sur la scène publique internationale ce dirigeant de crimes de guerre et de tentative de génocide, Moscou mettait en péril sa politique de rapprochement avec l'Ouest. Par ailleurs, en discréditant le président Saakashvili, un autre objectif de cette opération d'information était de l'isoler du peuple géorgien. Le message des médias russes distinguait alors le « criminel » Saakashvili du peuple géorgien, pour lequel le président Medvedov professait son amitié fraternelle. La Russie pouvait ainsi espérer un changement de régime, sans avoir à intervenir militairement sur le territoire géorgien.[180] Sans affirmer de lien causal, l'élection suivante, en 2012, a été remportée par le parti d'opposition qui a par la suite poursuivi en justice plusieurs membres du régime Saakashvili pour corruption.

En démontrant le manque de volonté de la part de l'OTAN de protéger ses partenaires dans la région, Moscou signalait au reste de ses voisins qu'une politique conciliante avec la Russie était désirable, au risque d'encourir le courroux du Kremlin.

[180] *Ibid*, p.20.

C. Les conséquences pour l'Ukraine de la révolution de *l'Euromaïdan* en 2014

> Ever since the dawn of the Ukraine crisis, the physical events were accompanied by an intense information struggle, a struggle to establish a narrative but also to mislead the opponents. Despite its likely origin at the top political level, this struggle differs from the pre-Internet and pre-globalization propaganda in some important aspects. Unlike propaganda during Soviet times, which relied heavily on narratives designed at the top level as well as on isolation, today's Russian IW incorporates the audience as a narrative-bearing and a narrative-developing factor.[181]
>
> - Jaitner et Mattsson

a. Guerre hybride et opération d'information

En Ukraine, une guerre hybride et une opération d'information se déroule conjointement. Une guerre hybride est un conflit armé dans lequel au moins une des parties en présence combine des forces conventionnelles et non-conventionnelles.[182] La saisie en 2014 de la Crimée par l'armée russe et la prise de contrôle de la région du Donbass par des groupes insurgés appuyés par des forces russes sans identifications officielles correspondent bien à la définition de guerre hybride.

En parallèle à cette guerre, Moscou se livrait à une lutte pour le contrôle du discours entourant cette opération militaire. Ainsi, les médias russes qualifiaient ces soldats sans identification de « personnes amicales » et de « bons citoyens ».[183] De plus, alors que la Russie avait imposé un ultimatum aux forces armées ukrainienne (soit rendre les armes ou quitter le territoire de Crimée), les médias russes ont rapidement déclaré une reddition massive de l'armée ukrainienne sans égard à l'exactitude des faits.[184] Cette tentative de contrôle s'est aussi étendue aux infrastructures de télécommunication ukrainiennes qui ont

---

[181] M. Jaitner et P. A. Mattsson (2015), « Russian Information Warfare of 2014 », dans M. Maybaum, A.-M. Osula et L. Lindström, *7th International Conference on Cyber Conflict: Architectures in Cyberspace*, Tallinn, NATO CCD COE Publications, p.46-47, https://ccdcoe.org/uploads/2018/10/CyCon_2015_book.pdf

[182] M. Galeotti (2016), *Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?,* Small Wars & Insurgencies, 27(2), p.286.

[183] M. Jaitner et P. A. Mattsson (2015), « Russian Information Warfare of 2014 », dans M. Maybaum, A.-M. Osula et L. Lindström, *7th International Conference on Cyber Conflict: Architectures in Cyberspace*, Tallinn, NATO CCD COE Publications, p.44, https://ccdcoe.org/uploads/2018/10/CyCon_2015_book.pdf

[184] *Ibid*, p.44.

été la cible de cyberattaques (DDoS)[185] et de perturbations physiques (saisi de bureaux et coupure de câbles de fibre optique).[186] La Russie veut ainsi faire valoir son message tout en empêchant son adversaire de faire valoir le sien.

b. Propagande et désinformation

Le soutien à cette guerre hybride n'est qu'une facette des opérations d'information menées par la Russie en Ukraine. Particulièrement depuis les manifestations de l'*Euromaïdan* en 2014, la Russie vise à déstabiliser l'Ukraine pour en faire un État non-fonctionnel et démontrer les conséquences néfastes de la démocratisation et du rapprochement avec l'Ouest.[187]

La Russie fait usage de nombreuses méthodes de transmission d'information pour disséminer à la fois sa propagande et sa désinformation. Des messages sont distribués dans les médias traditionnels, les médias sociaux, les sites internet et par message texte. Cette dernière méthode a souvent visé des soldats ukrainiens et des citoyens sur la ligne de front à l'est de l'Ukraine. Des messages visant à affecter négativement leur moral sont envoyés.[188]

La désinformation russe en Ukraine peut être divisée en cinq principaux thèmes : le fascisme; la peur et l'insécurité; l'interférence électorale; la corruption; la Russie n'est pas responsable de ce dont elle est accusée et la faute est attribuable aux pays de l'Ouest.[189] Ainsi, les autorités ukrainiennes sont régulièrement accusées de collaborer avec des groupes fascistes. Les citoyens sont bombardés d'informations faisant craindre une escalade de conflit militaire entre l'OTAN et la Russie, de même que sur la faiblesse de

[185] Distributed Denial of Service (en français : Déni de service distribué).
[186] *Ibid*, p.45.
[187] U.S. Senate Committee on Foreign Relations (2018), *PUTIN'S ASYMMETRIC ASSAULT ON DEMOCRACY IN RUSSIA AND EUROPE: IMPLICATIONS FOR U.S. NATIONAL SECURITY*, United States Senate, p.67, https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf
[188] T. C. Helmus, E. Bodine-Baron, A. Radin, M. Magnuson et al. (2018), *Russian Social Media Influence Understanding Russian Propaganda in Eastern Europe*, RAND Corporation p.16, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf
[189] EU vs Disinformation (2019), *Always Blame the West! – And Six Other Disinformation Trends*, European External Action Service East Stratcom Task Force, https://euvsdisinfo.eu/always-blame-the-west-and-six-other-disinformation-trends/

l'Ukraine dans un tel conflit. Il est répété que le processus électoral n'est pas crédible et malhonnête. Des informations véhiculent entre autres que des citoyens se voient refuser le droit de vote, que des votes sont achetés ou falsifiés, que la corruption sert à financer les campagnes électorales. Les Russes ne sont pas responsables des malheurs et des accidents. Par exemple, l'écrasement du vol MH17 était présenté comme étant la responsabilité de Kiev, et non de Moscou, pour ne pas avoir fermé l'espace aérien au-dessus du Donbass, province contrôlée par des groupes insurgés. Les pays de l'Ouest sont accusés d'intervenir dans les affaires internes des autres États, de les déstabiliser et d'être la cause de leurs maux.[190] De façon générale, le message est orienté vers l'instabilité, le chaos et l'insécurité causé par la révolution de *l'Euromaïdan* et le rapprochement avec l'Ouest. Ce message négatif est contrasté par celui de la stabilité et de la sécurité en Russie et dans certains pays ou provinces satellites comme la Crimée.[191]

Cette propagande et cette désinformation sont amplifiées par l'usage de *bots*. Ceux-ci vont partager, cliquer « j'aime » ou promouvoir du contenu sur les réseaux sociaux. Ainsi, un réseau de *bots* et de *trolls* prétendait être des patriotes ukrainiens et appelait à un troisième *Maïdan* contre le gouvernement. Les *bots* peuvent aussi augmenter l'impact de certaines pages ou personnalités virtuelles. L'audience de ces acteurs étant augmentée par des spectateurs (les *bots*) fictifs, leur visibilité sur les réseaux est magnifiée.[192] Ce contenu est de plus influencé par des commentateurs payés, les *trolls*. Ils opèrent dans les médias sociaux pour propager de la désinformation, promouvoir le discours officiel du Kremlin ou attaquer des opposants politiques.[193]

---

[190] *Ibid.*

[191] E. Lange-Ionatamishvili et S. Svetoka (2015), « Strategic Communications and Social Media in the Russia Ukraine Conflict », dans K. Geers (dir.), *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallinn, NATO CCD COE Publications, p.110-111, https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf

[192] M. Zhdanova et D. Orlova (2017), *Computational Propaganda in Ukraine: Caught between external threats and internal challenges,* Working Paper 2017.9, Project on Computational Propaganda, University of Oxford, p.12, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Ukraine.pdf

[193] *Ibid*, p.10 et 18.

c. Cyberespionnage

En plus d'une vaste campagne de désinformation, l'Ukraine est un laboratoire pour les cyberattaques russes. Les cybers capacités russes visent principalement la coercition politique, l'influence de l'opinion et la collecte d'information.[194] Ainsi, le Chef du *Computer Emergency Response Team* du gouvernement ukrainien explique que :

> Once the revolution began in February 2014, even ordinary Ukrainians became familiar with the combination of hacking and political activism, or 'hacktivism', in which the attackers seek to wage psychological war via the internet. Although many people were exhausted by the momentous political events that had shaken our country, it was hard to ignore the publication of allegedly leaked Ukrainian government documents detailing a secret, fascist government agenda.[195]

La Russie s'est aussi attaquée au suivi en direct du décompte des votes de l'élection de 2014 en rendant dysfonctionnel le site de la Commission électorale centrale (CEC). De plus, douze minutes avant la fermeture des bureaux de vote, les pirates informatiques ont affiché sur le site de la CEC une image du dirigeant du parti *Right Sector* (extrême-droite ultra-nationaliste) en affirmant faussement qu'il avait gagné l'élection. Cette image a immédiatement été montrée sur les réseaux de télévision russes.[196]

Des groupes de pirates informatiques comme APT29 et APT28 ciblent des organisations ou des individus conformément aux intérêts géopolitiques russes. Ils vont principalement voler des informations par l'hameçonnage ou l'ingénierie sociale. Ainsi, l'opération *Armageddon* a ciblé à partir de 2013 le gouvernement ukrainien, les forces policières et militaires. Cette opération visait à acquérir du renseignement tactique pouvant servir aux affrontements militaires sur le terrain. Ce cyberespionnage a probablement fourni un avantage militaire à la Russie dans son conflit avec l'Ukraine.[197] Ainsi, une supériorité stratégique dans les affrontements militaires et des avantages dans les affrontements socio-politiques sont à la fois poursuivis.

---

[194] J. A. Lewis (2015), « 'Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine », dans K. Geers (dir.), *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallinn, NATO CCD COE Publications, p.41, https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf

[195] N. Koval (2015), « Revolution Hacking », dans *ibid*, p.56.

[196] *Ibid*, p.56.

[197] J. Weedon (2015), « Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine », dans *ibid*, p.73.

d. Contrôle du messager

Afin d'affaiblir l'Ukraine, la corruption, la subversion et même les assassinats sont des outils utilisés par Moscou. Un rapport du Sénat américain considère d'ailleurs la corruption comme la principale vulnérabilité de l'Ukraine envers Moscou.[198] L'Ukraine se classe au 120e rang sur 180 du *Corruption Perception Index* de 2018.[199] Plusieurs sections du secteur privé et du gouvernement sont sous l'influence de Moscou. Le Service de Sécurité d'Ukraine (SBU), en particulier, contient des membres hauts placés ayant des liens problématiques avec la Russie.[200] Par ailleurs, le meurtre de critiques du régime russe et de journalistes est une technique dont se sert la Russie en Ukraine.[201] Par exemple, le meurtre du dissident russe Denis Voronenkov à Kiev en 2017 envoyait un message visant à faire taire les critiques du régime.[202]

De cette façon, le message, ceux le véhiculant ainsi que ceux sensé le protéger sont pris pour cibles.

---

[198] U.S. Senate Committee on Foreign Relations (2018), *PUTIN'S ASYMMETRIC ASSAULT ON DEMOCRACY IN RUSSIA AND EUROPE: IMPLICATIONS FOR U.S. NATIONAL SECURITY*, United States Senate, p.69, https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

[199] Transparency International (2019), *Corruption Perception Index 2018*, https://www.transparency.org/cpi2018

[200] O. Ustinova et S. Pifer (20129), *Time to play hardball on reforming Ukraine's Security Service*, Atlantic Council, https://www.atlanticcouncil.org/blogs/ukrainealert/time-to-play-hardball-on-reforming-ukraine-s-security-service

[201] U.S. Senate Committee on Foreign Relations (2018), *PUTIN'S ASYMMETRIC ASSAULT ON DEMOCRACY IN RUSSIA AND EUROPE: IMPLICATIONS FOR U.S. NATIONAL SECURITY*, United States Senate, p.1, https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

[202] I. Webb (2017), *Brazen Murder in Kiev Chills Russia's Dissidents in Ukraine*, Foreign Policy, https://foreignpolicy.com/2017/03/28/brazen-murder-in-kiev-chills-russias-dissidents-in-ukraine/

D. La désinformation en Suède depuis 2014

> An increasing amount of disinformation, forged telegrams and fake news items have surfaced in the Swedish information landscape. These developments have taken place in the context of a deteriorated security situation in the wider Baltic region, following Russia's annexation of Crimea in February 2014.[203]
>
> - Kragh et Asberg

a. La Suède et l'OTAN

La Suède est régulièrement décrite comme étant le « partenaire numéro 1 »[204] de l'OTAN. Bien que la Suède maintienne une position traditionnelle de neutralité et ne soit pas membre de l'organisation, elle s'est à plusieurs reprises alignée du côté des pays de l'OTAN. Sa contribution à l'opération *Unified Protector* en Lybie durant l'année 2011 a particulièrement été remarquée. En 2016, la Suède signait avec l'OTAN un accord de coopération permettant de faciliter les opérations sur le territoire suédois durant les entraînements ou dans l'éventualité d'un conflit.[205] Elle a de plus participé à plusieurs exercices conjoints, dont *Trident Juncture* en 2018, ce qui a constitué un irritant pour la Russie.[206] La participation à l'OTAN des pays d'Europe du Nord, à l'image de celle des pays de l'Europe de l'Est, constitue une préoccupation constante pour la Russie, lui faisant craindre un encerclement, ainsi qu'un isolement militaire et diplomatique. La Russie intervient à plusieurs niveaux dans le débat public en Suède concernant le rapport du pays à l'OTAN. Suite au réalignement de l'Ukraine vers l'Ouest en 2014, les activités de désinformation en Suède ont augmentées.[207]

---

[203] M. Kragh et S. Åsberg (2017), *Russia's strategy for influence through public diplomacy and active measures: the Swedish case*, Journal of Strategic Studies, 40(6), p.773, https://www.tandfonline.com/doi/full/10.1080/01402390.2016.1273830

[204] A.-S. Dahl (2012), *Partner number one or NATO ally twenty-nine? Sweden and NATO post-Lybia,* Research Division – Nato Defense College, No.82, p.1, https://www.files.ethz.ch/isn/153549/rp_82.pdf

[205] C. Duxbury (2016), *Sweden Ratifies NATO Cooperation Agreement*, The Wall Street Journal, https://www.wsj.com/articles/sweden-ratifies-nato-cooperation-agreement-1464195502

[206] Baltic Monitor (2018), *Russia reacts to Trident Juncture 18*, Warsaw Institute, https://warsawinstitute.org/russia-reacts-trident-juncture-18/

[207] M. Kragh et S. Åsberg (2017), *Russia's strategy for influence through public diplomacy and active measures: the Swedish case*, Journal of Strategic Studies, 40(6), pp.781, https://www.tandfonline.com/doi/full/10.1080/01402390.2016.1273830

b. Cyberattaque

Le 19 mars 2016, une cyberattaque a mis hors ligne pendant 3 heures au moins sept médias majeurs de Suède. L'attaque était de type DDoS et provenait de la Russie, selon une enquête de l'unité de cyber crimes de la police nationale suédoise.[208] Cette attaque est survenue deux jours après que la Suède ait dévoilé une nouvelle doctrine militaire annonçant une stratégie plus agressive et orientée vers un potentiel conflit avec la Russie.[209] L'attaque a été revendiquée sur Twitter par un utilisateur nommé J, @_notJ qui écrivait : « this is what happens when you spread false propaganda »[210]. Il s'agissait probablement d'une tentative d'intimidation de la Suède en réaction à son rapprochement avec les États-Unis et l'OTAN.[211]

c. Propagande médiatique

La chaîne d'information *Sputnik* a offert une version suédoise de son site internet entre avril 2015 et mars 2016. Une étude suédoise a catégorisé les 3963 articles publiés en 2015 selon 10 thèmes pour en définir la trame narrative dominante.[212]

[208] E. Brattberg et T. Maurer (2018), *RUSSIAN ELECTION INTERFERENCEL Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, p.24, https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf

[209] Defense News (2016), *Sweden Adopts Tougher Military Strategy Doctrine*, https://www.defensenews.com/global/europe/2016/03/17/sweden-adopts-tougher-military-strategy-doctrine/

[210] Radware (2016), *Attack on Sweden's Media*, https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/sweden-attack-threat-alert/

[211] E. Brattberg et T. Maurer (2018), *RUSSIAN ELECTION INTERFERENCE: Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, p.24, https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf

[212] M. Kragh et S. Åsberg (2017), *Russia's strategy for influence through public diplomacy and active measures: the Swedish case*, Journal of Strategic Studies, 40(6), pp.782, https://www.tandfonline.com/doi/full/10.1080/01402390.2016.1273830

Thèmes	Nombres de publications	Pourcentage des articles totaux (%)
Crise à l'Ouest	705	17.79
Image positive de la Russie	643	16.23
Agressivité de l'Ouest	499	12.59
Image négative des pays perçus comme étant dans la sphère d'influence de l'Ouest	424	10.7
L'Ouest est malicieux	309	7.8
Sympathie internationale et coopération avec la Russie	304	7.67
Échec des politiques de l'Ouest	112	2.83
Divisions parmi l'alliance de l'Ouest	72	1.82
Intérêts humains / piège à clics	276	6.96
Nouvelles diverses et inclassables	619	15.62

Cette étude démontre que la majorité du contenu publié par *Sputnik* projette une image négative de l'Ouest et favorable de la Russie.

Ces articles ont aussi été catégorisés selon les pays auxquels ils font référence.[213]

Pays ou organisation	Nombre de publications
États-Unis	1018
Ukraine	882
Allemagne	390
France	360
Finlande	332
Suède	**303**

Selon cette étude, deux possibilités expliqueraient le peu d'attention accordé à la Suède dans cette liste par rapport aux autres pays malgré que le média soit en langue

[213] *Ibid*, p.784.

suédoise. Premièrement, la Suède n'était peut-être pas une priorité et l'équipe éditoriale ne possédait pas les ressources nécessaires pour couvrir les affaires intérieures. Deuxièmement, les critiques envers l'OTAN et l'Union Européenne (EU) (qui constituent environ la moitié des articles) serait l'histoire dominante que la Russie veut communiquer à l'auditoire suédois, tout comme au reste de l'auditoire européen.[214]

En traitant de l'actualité sous cet angle, ces médias visent à renforcer les sentiments d'opposition aux « élites » de certains groupes spécifiques. Que ce soit les mouvements de gauche, pour la paix, pour l'environnement, contre les OGM, conspirationniste, d'extrême-droite ou populistes, les trames narratives sont développées de telle sorte à rejoindre les préoccupations préexistantes de groupes cibles.[215] C'est ainsi que les articles concernant la Suède traitaient principalement des migrations, le sujet dominant du moment dans l'UE, et selon un thème qui impliquait la chute imminente de l'Union Européenne.[216] Ceci était de nature à renforcer les inquiétudes de la population, ainsi que les mouvements de l'extrême-droite suédoise dont une partie est favorable au Kremlin, telle que l'organisation Résistance Nordique.[217]

d. Désinformation

Alors que la désinformation précédait la version suédoise de *Sputnik* et s'est poursuivie après sa fermeture, ses thèmes continuent de renforcer les inquiétudes de certains suédois en présentant un pays au bord de la guerre civile, une société immorale et qui s'est volontairement islamisée.[218] Entre 2014 et 2016, 26 faux documents ont été répertoriées dans l'environnement informationnel suédois. Ces documents décrivent des conspirations provenant de l'OTAN, de l'Allemagne, de l'Ukraine, de politiciens suédois ou d'organisation terroristes qui effectuent des ententes secrètes de nature à remettre en

[214] *Ibid*, p.782-784.
[215] *Ibid*, p.788-789.
[216] *Ibid*, p.788.
[217] *Ibid*, p.802.
[218] EU vs Disinformation (2018), *In Sweden, Resilience is Key to Combatting Disinformation*, European External Action Service East Stratcom Task Force, https://euvsdisinfo.eu/in-sweden-resilience-is-key-to-combatting-disinformation/

question la confiance envers l'information transmise par les médias traditionnels et les politiciens.[219]

Malgré cela, une étude de 2015 démontrait que la majorité des suédois ont une confiance élevée dans leurs médias traditionnels. Cependant, ce niveau de confiance descendait drastiquement par rapport au sujet des migrants. En effet, 54% des répondants au sondage affirmaient qu'ils étaient en accord ou partiellement en accord avec l'affirmation selon laquelle les médias ne produisent pas de l'information exacte sur les enjeux entourant l'immigration.[220]

L'élection de 2018 a été particulièrement significative du point de la vue de la désinformation russe puisque l'accession à l'OTAN en tant que pays membre était soutenue par le bloc de quatre partis de l'opposition.[221] Du contenu partagé sur Twitter concernant la politique et les élections, au moins 11% a été généré par des *bots* (c'est-à-dire un partage automatisé) et un minimum de 6% des comptes étaient des *bots*.[222] Une autre étude a démontré que les fausses nouvelles ont représenté 22% des liens partagés par les utilisateurs. La majorité de celles-ci provenaient toutefois de sources intérieures, et non de pays étrangers.[223] Les fausses nouvelles générées ou partagées automatiquement promulguaient des opinions globalement en faveur de points de vue nationalistes, autoritaires, traditionnalistes et critiques de l'immigration. Ils appuyaient largement le parti

[219] M. Kragh et S. Åsberg (2017), *Russia's strategy for influence through public diplomacy and active measures: the Swedish case*, Journal of Strategic Studies, 40(6), pp.791, https://www.tandfonline.com/doi/full/10.1080/01402390.2016.1273830

[220] F. Hedman, F. Sivnert, B. Kollanyi et al. (2018), *News and Political Information Consumption in Sweden: Mapping the 2018 Swedish General Election on Twitter*, DATA MEMO 2018.3, Project on Computational Propaganda, University of Oxford, p.2, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/09/Hedman-et-al-2018.pdf

[221] A. Wieslander (2018), *Will Sweden's Elections Lead to NATO Membership?,* Atlantic Council, https://www.atlanticcouncil.org/blogs/new-atlanticist/will-sweden-s-elections-lead-to-nato-membership

[222] J. Fernquist, L. Kaati, R. Schroeder et al. (2018), *Bots and the Swedish election: A study of automated accounts on Twitter*, Swedish Defence Research Agency (FOI), p.3, https://www.foi.se/rapportsammanfattning?reportNo=FOI%20MEMO%206466

[223] F. Hedman, F. Sivnert, B. Kollanyi et al. (2018), *News and Political Information Consumption in Sweden: Mapping the 2018 Swedish General Election on Twitter*, DATA MEMO 2018.3, Project on Computational Propaganda, University of Oxford, p.5, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/09/Hedman-et-al-2018.pdf

des Démocrates Suédois, caractérisé comme étant à l'extrême droite et étaient critiques des partis principaux de Suède, soit les Sociaux-Démocrates et les Conservateurs.[224]

e. Manipulation de l'information concernant les sous-marins russes en eaux suédoises

Un exemple en particulier a eu une forte médiatisation en Suède. Alors qu'en octobre 2014 le renseignement électronique de Suède avait détecté des communications radios sur un canal d'urgence russe et qu'un citoyen déclarait aux autorités avoir aperçu un sous-marin, la marine suédoise s'est mise à la recherche de ce prétendu sous-marin russe qui aurait violé les eaux territoriales suédoises. Les autorités de Russie ont nié l'incident et prétendus que le navire aurait été hollandais. Les médias russes se sont emparés de l'histoire en ajoutant notamment que cela aurait pu être un simple animal et en référant à cette histoire comme une recherche pour un sous-marin fantôme. Alors que l'enquête de la marine suédoise n'a mené à aucune découverte, les médias russes semblaient avoir eu raison.[225]

Par la suite, d'autres informations ambigües ont émergé à propos d'une recherche semblable en 2015. Un article de 2016 sur le site d'un média public suédois déclarait que le sous-marin était en fait probablement d'origine allemande et non russe, selon des sources anonymes et non corroborées au sein du gouvernement. Une information niée par le ministère des Affaires étrangères allemand. Une situation semblable est survenue en août 2015 lorsqu'une compagnie privée de plongée sous-marine a affirmé avoir découvert l'épave d'un sous-marin russe dans les eaux suédoises. Une fois la confusion autour de la nouvelle résorbée, il s'est avéré qu'il s'agissait d'une ancienne épave de 1916. Il a par la

[224] J. Fernquist, L. Kaati, R. Schroeder et al. (2018), *Bots and the Swedish election: A study of automated accounts on Twitter*, Swedish Defence Research Agency (FOI), p.12, https://www.foi.se/rapportsammanfattning?reportNo=FOI%20MEMO%206466

[225] E. Braw (2018), *How to Deal With Russian Information Warfare? Ask Sweden's Subhunters*, Defense One, https://www.defenseone.com/ideas/2018/04/how-deal-russian-information-warfare-ask-sweden/147154/

suite été révélé que cette expédition avait été financée par un individu privé russe, qui avait offert un bateau à cette équipe et fourni les coordonnées exactes de l'épave.[226]

Cet ensemble d'informations confuses ou fausses ont été reprises par les médias *Russia Today* (*RT)* et *Sputnik* pour faire paraître les autorités suédoises comme étant à la fois obsédées par ces histoires de sous-marins russes et russophobes.[227] Le public suédois reste divisé quant à savoir si des sous-marins russes font réellement intrusion dans les eaux suédoises.[228] Un général suédois retraité explique que : « The Russian tactic is to put on a blank face and sow uncertainty among everyone who doesn't have 100-percent-certain evidence. And the Russians always try to make the other side look like idiots. »[229] Ce message fonctionne ainsi à plusieurs niveaux. Il montre à la fois aux Suédois les capacités militaires russes et leurs capacités à influencer l'opinion publique. De plus, il crée une confusion dans la population quant à la politique de leur gouvernement par rapport à la Russie, semblant indiquer une à russophobie irrationnelle.

[226] M. Kragh et S. Åsberg (2017), *Russia's strategy for influence through public diplomacy and active measures: the Swedish case*, Journal of Strategic Studies, 40(6), pp.799-801, https://www.tandfonline.com/doi/full/10.1080/01402390.2016.1273830
[227] *Ibid*, p.801.
[228] E. Braw (2018), *How to Deal With Russian Information Warfare? Ask Sweden's Subhunters*, Defense One, https://www.defenseone.com/ideas/2018/04/how-deal-russian-information-warfare-ask-sweden/147154/
[229] *Ibid.*

E. Le référendum du *Brexit* au Royaume-Uni en 2016

> The electorate's decision to leave the European Union in June 2016 suited the Kremlin, because it weakened the EU overall and made exits by other states more likely. (…) In particular, the UK's nuclear deterrent and its position as a leading hawk on the question of EU sanctions on Russia mark it out as a target for Russian "active measures."[230]
>
> - Neil Barnett

a. Financement de la campagne référendaire

La campagne *Leave.EU*, en faveur de la sortie du Royaume-Uni de l'Union Européenne (*Brexit*), a reçu un financement total de 24.4 millions de livres (£). Le tiers de ce montant provenait de Arron Banks, qui a fourni, sous forme des dons ou de prêts, 8.1 millions de livres (£).[231] Toutefois, la source de ce financement est remise en question, alors que des doutes sérieux ont été soulevés à la fois sur le niveau réel des avoirs de M. Banks et sur l'origine de l'argent donné.[232] Cet argent est suspecté de provenir de fonds étrangers, ce qui rendrait cette contribution problématique du point de vue des lois britannique sur le financement électoral. Le *National Crime Agency* mène présentement une enquête sur l'origine de ces fonds.

Les liens de M. Banks avec la Russie rendent possible qu'une part du financement pour la campagne pro-*Brexit* provienne de Moscou. En effet, le comité britannique chargé de faire enquête sur la désinformation et les fausses nouvelles a rapporté que M. Banks avait trompé le comité sur la fréquence de ses contacts avec l'ambassade russe.[233] Il a

---

[230] A. Polyakova, M. Laruelle, S. Meister et N. Barnett (2016), *THE KREMLIN'S TROJAN HORSES: Russian Influence in France, Germany, and the United Kingdom*, DINU Patriciu Eurasia Center – Atlantic Council, p.18, https://www.atlanticcouncil.org/images/publications/The_Kremlins_Trojan_Horses_web_0228_third_edition.pdf

[231] A. Payne et W. Martin (2017), *The 21 biggest donors to the Brexit campaign*, Business Insiders, https://www.businessinsider.com/twenty-one-biggest-donors-to-the-leave-brexit-campaign-2017-5

[232] The Digital, Culture, Media and Sport Committee (2019), *Disinformation and 'fake news': Final Report*, U.K. House of Commons, p.74, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf

[233] *Ibid*, p.74.

notamment rencontré l'ambassadeur de Russie et discuté de potentielles ententes concernant des mines d'or et de diamant.[234] Ils ajoutent que M. Banks a quitté son entretien avec le comité pour éviter que le contenu de ces rencontres soit scruté. Il n'est pas clair s'il a profité des ententes commerciales discutées lors de ces rencontres.

Par ailleurs, il est bien connu que de vastes sommes provenant de Russie sont entrées dans le marché immobilier britannique. Des documents révélaient que les banques britanniques avaient traité 740 millions de dollars ($) d'un complot visant à blanchir au moins 20 milliards de dollars illicites provenant de Russie entre 2010 et 2014. Cette disponibilité des fonds russes au Royaume-Uni fait craindre au sénat américain qu'une variété d'acteurs y soient vulnérables à l'influence du Kremlin.[235]

b. Propagande médiatique

Bien que le gouvernement russe se soit officiellement prononcé comme étant neutre par rapport à l'issue du référendum de 2016, les médias russes ont clairement démontré un biais en faveur de la sortie de l'Union Européenne (UE).[236] Entre le 1ier et le 8 février, *Sputnik* a publié 14 articles concernant le *Brexit*. Huit de ces titres était négatifs. Ils concernaient des critiques de l'entente que David Cameron avait négociée avec l'UE. Cinq articles étaient simplement factuels et un article rapportait un commentaire positif de la Banque d'Angleterre, mais avec une tournure faisant paraître une inquiétude à venir. Aucun article favorable au maintien dans l'UE n'est paru.[237]

Suivant ce même biais, *RT* et *Sputnik* ont cité d'une façon disproportionnée les partisans de la sortie de l'UE. De plus, lorsque des partisans du maintien dans l'UE étaient cités, beaucoup moins d'espace de texte leur était alloué. Des articles entiers ou des

[234] The Digital, Culture, Media and Sport Committee (2018), *Disinformation and 'fake news': Interim Report*, U.K. House of Commons, p.50, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf
[235] U.S. Senate Committee on Foreign Relations (2018), *PUTIN'S ASYMMETRIC ASSAULT ON DEMOCRACY IN RUSSIA AND EUROPE: IMPLICATIONS FOR U.S. NATIONAL SECURITY*, United States Senate, p.117, https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf
[236] Ibid, p.118.
[237] B. Nimmo (2016), *Putin's media are pushing Britain for the Brexit*, The Interpreter, http://www.interpretermag.com/putins-media-are-pushing-britain-for-the-brexit/

entrevues étaient consacrées aux partisans du *Brexit*, tandis qu'aucun équivalent n'était accordé au camp opposé. De plus, durant les entrevues avec les partisans en faveur du *Brexit*, les questions posées étaient formulées de telle sorte à renforcer ce biais en faveur de la sortie de l'UE. Ainsi, un journaliste de *RT* demandait en entrevue: « He [Cameron] is, of course, a PR man, but on the other hand, do you think the point is that he hasn't been doing the PR that well this time? [ou bien] Why do you think the BBC is so pro-remaining in the European Union?'' ». [238]

c. Désinformation dans les médias sociaux

Facebook

Par suite de l'ingérence russe dans les élections américaines, Twitter et Facebook ont rendus disponibles des données concernant les faux comptes russes ayant été utilisés pour propager de la désinformation durant la campagne électorale aux Etats-Unis. Le comité britannique chargé d'étudier la question de l'ingérence russe a fait des demandes répétées, et longtemps sans réponses, à Facebook pour obtenir les données équivalentes pour le référendum britannique.[239] Lorsque des données ont été fournies au comité, elles indiquaient seulement que la *Internet Research Agency* (*IRA*)[240] avait achetée 3 publicités pour la somme de 0.97$ durant la période officielle de la campagne référendaire. Ceci n'incluait pas les publications non payées et donc la majorité de l'activité potentielle de l'IRA sur Facebook. De plus, aucune enquête n'a été menée sur les organisations de *trolls* au-delà de l'*IRA*. En étendant la recherche, il a été déterminé que des publicités anti-

[238] *Ibid.*

[239] The Digital, Culture, Media and Sport Committee (2019), *Disinformation and 'fake news': Final Report*, U.K. House of Commons, p.72, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf

[240] L'*IRA* est une « ferme de trolls ». Elle est une organisation russe dont la mission est la promotion de fausses nouvelles et de manipulation du discours dans les réseaux sociaux. Son dirigeant est un proche de Vladimir Poutine. Pour plus de précisions sur cette organisation, voir : A. Dawson et M. Innes (2019), *How Russia's Internet Research Agency Built its Disinformation Campaign*, The Political Quarterly, 90(2), p.246-247, https://onlinelibrary.wiley.com/doi/full/10.1111/1467-923X.12690

immigrants avait été placées par l'agence russe en octobre 2015 pour un montent de 66 livres (£).[241]

Ainsi, les données disponibles indiquent un très faible niveau d'activité sur Facebook durant la campagne référendaire. Par contre, les données sont partielles et très limitées. Ce comité concluait que les représentants de Facebook ayant été interrogés ont « deliberately misled the Committee or they were deliberately not briefed by senior executives at Facebook about the extent of Russian interference in foreign elections. »[242]

Twitter

Les données rendues disponibles par Twitter sont plus concluantes. Suite aux élections américaines de 2016, Twitter a publié une liste de 2,752 comptes contrôlés par des opérateurs russes. Des chercheurs ont découvert qu'entre le 29 août 2015 et le 3 octobre 2017, 419 de ces comptes avaient été utilisés pour publier du contenu concernant le *Brexit*, pour un total de 3,485 tweets sur le sujet. Cinquante-trois pourcent du contenu a été généré par des humains (référés en tant que *trolls*), tandis que le 47% restant l'a été par des *bots* (soit du contenu automatisé). La majorité de ces comptes ont été créés en 2013 ou 2014.[243] Par ailleurs, « the behaviour of the accounts altered radically on the day of the referendum, shifting from generalised disruptive tweeting to retweeting each other in order to amplify content produced by other troll accounts. »[244] Ainsi, pour la seule journée du vote référendaire, le 23 juin 2016, 400 *tweets* (sur les 3,485) ont été publiés. Ils concernaient massivement le *Brexit*. La vaste majorité (97.73%) était toutefois des re-*tweets*, soit un partage d'une publication précédente et non du contenu original.[245]

---

[241] The Digital, Culture, Media and Sport Committee (2018), *Disinformation and 'fake news': Interim Report*, U.K. House of Commons, p.45, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf

[242] The Digital, Culture, Media and Sport Committee (2019), *Disinformation and 'fake news': Final Report*, U.K. House of Commons, p.72, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf

[243] C. Llewellyn, L. Cram, A. Favero et R. L. Hill (2019), *For Whom the Bell Trolls: Troll Behaviour in the Twitter Brexit Debate*, JCMS: Journal of Common Market Studies, p.1-4, https://onlinelibrary.wiley.com/doi/full/10.1111/jcms.12882

[244] *Ibid*, p.1.

[245] *Ibid*, p.6-7.

Une autre recherche utilisant un plus grand nombre de *tweets* comme base de données est aussi arrivée à la conclusion que le jour du vote a vu une augmentation massive de tweets concernant le *Brexit* provenant d'utilisateurs de langue russe. En comparaison, les tweets concernant les élections américaines de 2016 avaient un volume relativement constant trente jours avant et après les élections.[246]

Durant la période de juin 2016, celle de la campagne référendaire sur le *Brexit*, les *tweets* étaient largement en faveur de la sortie de l'Union Européenne. Toutefois, sur l'ensemble de la période 2016-2017, les *tweets* pouvaient à la fois prendre une position neutre, en faveur ou contre le *Brexit*. Cette répartition des opinions fait conclure aux chercheurs que l'objectif visé était soit de faire paraître ces comptes plus réalistes (en publiant du contenu d'actualité) ou d'augmenter l'instabilité et les perturbations dans le climat socio-politique.[247] À l'exception de la journée du vote, le nombre de *tweets* par jour était très faible. Les journées de grandes activités correspondent à des événements d'importance, comme la visite de Mme May à Mme Merkel par exemple.[248]

De plus, ces *tweets* ont parfois été repris par des médias officiels. Les médias du Royaume-Uni ont cité à au moins 73 reprises des *tweets* provenant de comptes appartenant à des *trolls* russes.[249] Certaines reprises ne contenaient que du contenu léger et apolitique, mais d'autres reprenaient des réactions de fausses organisations ou de faux individus.[250] Aucun de ces exemples ne traitait explicitement du *Brexit*, mais cela témoigne de la capacité de pénétration des médias officiels par les faux comptes russes.

---

[246] Y. Gorodnichenko, T. Pham et O. Talavera (2018), *Social media, sentiment and public opinions: Evidence from #Brexit and #USElection*, National Bureau of Economic Research, Working Paper No. 24631, p.9, https://rahwebdav.swan.ac.uk/repec/pdf/wp2018-01.pdf

[247] Llewellyn, Cram, Favero et Hill, *For Whom the Bell Trolls: Troll Behaviour in the Twitter Brexit Debate*, JCMS: Journal of Common Market Studies, p.8, https://arxiv.org/pdf/1801.08754.pdf.

[248] *Ibid*, p.6.

[249] En se basant sur les données des 2,752 comptes de l'*IRA* fournis par Twitter.

[250] A. Hern, P. Duncan et H. Bengtsson, *Russian 'troll army' tweets cited more than 80 times in UK media*, The Guardian, https://www.theguardian.com/media/2017/nov/20/russian-troll-army-tweets-cited-more-than-80-times-in-uk-media

F. L'élection présidentielle américaine de 2016

> For years, Vladimir Putin's government has engaged in a relentless assault to undermine democracy and the rule of law in Europe and the United States. (…) If the United States fails to work with urgency to address this complex and growing threat, the regime in Moscow will become further emboldened. It will continue to develop and refine its arsenal to use on democracies around the world.[251]
>
> - Benjamin L. Cardin

a. Collecte d'informations

Au moins à partir de 2014, l'*Internet Research Agency* (*IRA*) a effectué une collecte d'informations sur la situation socio-politique américaine. En juin et en novembre 2014, des membres de cette organisation ont voyagé aux États-Unis dans le but de collecter des informations de nature sociale, culturelle et politique. Les employés de l'*IRA* ont aussi étudié des groupes socio-politiques sur les réseaux sociaux en notant leur taille, la fréquence de leurs publications et le niveau de réponse de la part de l'audience. Ils ont de plus prétendu être des citoyens américains afin de contacter des représentants de groupes politiques ou des activistes sociaux pour collecter de l'information sur leur stratégie d'influence.[252] Cette dimension de l'opération avait comme but de poser les bases d'une stratégie d'ingérence dans les médias sociaux ciblée sur les divisions et les vulnérabilités de la société américaine. Cette stratégie est inspirée des techniques du marketing numérique, semblable à une campagne publicitaire multiplateforme.[253]

---

[251] U.S. Senate Committee on Foreign Relations (2018), *PUTIN'S ASYMMETRIC ASSAULT ON DEMOCRACY IN RUSSIA AND EUROPE: IMPLICATIONS FOR U.S. NATIONAL SECURITY*, United States Senate, p.IV, https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

[252] R. S. Mueller III (2018), *UNITED STATES OF AMERICA v. INTERNET RESEARCH AGENCY LLC [and other Defendants]*, United States Department of Justice, p.12-13 https://www.justice.gov/file/1035477/download?fbclid=IwAR3YArxy3bTNVUWrWaI9kZpo34dF_9isYZfG5veSz2MB_OfGz9vZEkkAr3s

[253] P. N. Howard, B. Ganesh et D. Liotsiou (2018), *The IRA, Social Media and Political Polarization in the United States, 2012-2018*, Working Paper 2018.2 Project on Computational Propaganda, University of Oxford, p.8, https://comprop.oii.ox.ac.uk/research/ira-political-polarization/

b. Fausses identités virtuelles

En utilisant ces informations, l'*IRA* a créé des personnalités d'influence virtuelles. L'objectif était de créer des leaders américains de l'opinion publique fictifs qui pourraient provoquer des événements et des sentiments parmi la population américaine réelle.[254] La création de ces comptes et leurs premières publications remonte parfois à 2013, mais leurs activités ont pris une ampleur significative dès le début de 2014. Les premiers comptes ont été créés sur Twitter et ils se sont répandus sur les autres plateformes vers la fin de 2014.[255] Les publications sur ces comptes visaient à stimuler les sentiments d'insatisfaction sur des sujets variés de la politique, de la société ou de l'économie. Ces interventions appuyaient aussi des mouvements radicaux. Ces personnalités fictives pouvaient prétendre représenter des groupes catégorisés à gauche comme à droite, ainsi que des communautés ethniques (afro-américaines, autochtones), sociales (homosexuelles, environnementales, immigrations), religieuses (musulmanes) ou géographiques (texanes, sudistes). En 2016, la taille de plusieurs de ces fausses organisations avait cru jusqu'à inclure des centaines de milliers d'abonnés.[256]

Ces groupes ont notamment influencé des individus à participer à des manifestations, de même qu'à des contre-manifestations sur des sujets controversés comme l'immigration. Facebook a dévoilé que 13 pages contrôlées par des agents russes ont promus 130 rassemblements. Ces pages pouvaient rejoindre jusqu'à 126 millions

[254] R. S. Mueller III (2018), *UNITED STATES OF AMERICA v. INTERNET RESEARCH AGENCY LLC [and other Defendants]*, United States Department of Justice, p.14 https://www.justice.gov/file/1035477/download?fbclid=IwAR3YArxy3bTNVUWrWaI9kZpo34dF_9isYZfG5veSz2MB_OfGz9vZEkkAr3s

[255] P. N. Howard, B. Ganesh et D. Liotsiou (2018), *The IRA, Social Media and Political Polarization in the United States, 2012-2018*, Working Paper 2018.2 Project on Computational Propaganda, University of Oxford, p.9, https://comprop.oii.ox.ac.uk/research/ira-political-polarization/

[256] R. S. Mueller III (2018), *UNITED STATES OF AMERICA v. INTERNET RESEARCH AGENCY LLC [and other Defendants]*, United States Department of Justice, p.14 https://www.justice.gov/file/1035477/download?fbclid=IwAR3YArxy3bTNVUWrWaI9kZpo34dF_9isYZfG5veSz2MB_OfGz9vZEkkAr3s

d'Américains.[257] De cette façon, des activistes américains, notamment concernant les enjeux afro-américains, ont collaboré sans le savoir avec les fausses organisations russes.[258]

c. Désinformation

Les activités de l'*IRA* avaient comme objectifs de nourrir les divisions sociales et d'influencer la société américaine sur des enjeux spécifiques.[259] La campagne de désinformation sur les médias sociaux de l'*IRA* ne visait que peu Trump et Clinton directement. En effet, seul un faible pourcentage de ces publications concernait l'un ou l'autre des candidats. Des données collectées entre 2014 et 2017 indiquent que, sur les 61,483 publications Facebook, seulement 2.9% mentionnaient Clinton et 4.2% mentionnaient Trump; sur les 116,205 publications Instagram, 6.8% mentionnent Clinton et 11.3% Trump; finalement sur les 10,401,029 tweets 1.9% mentionnent Clinton et 4.1% Trump.[260]

Toutefois, parmi les messages visant la droite américaine, l'*IRA* exprimait dès le début de 2015 une claire préférence pour Donald Trump. Ainsi, durant les primaires républicaines, des messages dénigrants apparaissaient contre Cruz, Rubio et Bush, tandis que d'autres promouvaient Trump. Par ailleurs, parmi les messages visant la gauche américaine, l'*IRA* publiait en parallèle du contenu négatif à propos de Trump. Contrairement à cette polarisation autour de Trump, la totalité du contenu publié sur Clinton était négatif, autant dans les groupes de gauche, de droite ou dans les communautés afro-américaines.[261]

---

[257] Shane (2018), *How Unwitting Americans Encountered Russian Operatives Online*, The New York Times, https://www.nytimes.com/2018/02/18/us/politics/russian-operatives-facebook-twitter.html
[258] B. Ross, M. Mosk, R. Kreider et al. (2017), *Russian internet trolls sought to co-opt unwitting American activists*, ABC News, https://abcnews.go.com/Politics/russian-internet-trolls-sought-opt-unwitting-american-activists/story?id=50570832
[259] P. N. Howard, B. Ganesh et D. Liotsiou (2018), *The IRA, Social Media and Political Polarization in the United States, 2012-2018*, Working Paper 2018.2 Project on Computational Propaganda, University of Oxford, p.39, https://comprop.oii.ox.ac.uk/research/ira-political-polarization/
[260] R. DiResta, J. Albright, B. Johnson et al. (2018), *The Tactics & Tropes of the Internet Research Agency*, New Knowledge, p.76, https://cdn2.hubspot.net/hubfs/4326998/ira-report-rebrand_FinalJ14.pdf
[261] *Ibid*, p.80-81.

Une semaine avant le scrutin, la stratégie de l'*IRA* a évoluée et s'est portée sur deux thèmes distincts concernant d'un côté les groupes de gauche et afro-américains et de l'autre les groupes de droite. À droite, la stratégie a été d'accentuer les sentiments de suspicion et de colère. L'*IRA* faisait circuler des histoires de fraude électorale, de complots, de votes illégaux et des appels à la rébellion advenant une victoire ''volée'' par Clinton. À gauche, les publications au sujet de l'aliénation sociale et la brutalité policière se sont poursuivies sans changement. Cependant, à quelques jours du vote, elles ont été mélangées à des appels à ne pas aller voter, à rester à la maison, à des propos sur l'absence de préoccupations des candidats pour les afro-américains, à des tirades contre *l'establishment*, ou des incitations à voter pour d'autres candidats que Clinton. De façon générale, les informations suggéraient des émotions actives incitant à la participation pour les groupes de droite et des émotions passives, de résignation ou de découragement à gauche afin d'inciter à ne pas participer au scrutin.[262]

d. Cyberespionnage et révélations embarrassantes

Parallèlement aux activités sur les médias sociaux, les services de renseignement russes ont effectué du piratage informatique afin d'obtenir des informations privées sur des organisations politiques ou des candidats aux élections.[263] En juillet 2015, le renseignement russe a réussi à pénétrer le réseau informatique du *Democratic National Committee* (DNC). Il a conservé cet accès au moins jusqu'en juin 2016. De plus, un pirate informatique a accédé au courriel du président de la campagne de Clinton, John Podesta, par le moyen d'une opération d'hameçonnage[264]. Ces deux piratages ont été les plus médiatiquement visibles. Toutefois, des centaines, voire plus d'un millier d'organisations américaines gouvernementales et non-gouvernementales ont été visées par ces opérations

[262] *Ibid*, p.83.
[263] Office of the Director of National Intelligence – DNI (2017), *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, United States Government, p.2, https://www.dni.gov/files/documents/ICA_2017_01.pdf
[264] Le hameçonnage est une activité consistant notamment à obtenir accès à un serveur sécurisé par le moyen d'un message trompeur visant à convaincre la cible de donner elle-même son mot de passe.

d'hameçonnage.[265] Les cibles incluaient aussi des organisations associées au Parti républicain.

Les documents collectés contenaient parfois des informations sensibles, compromettantes ou embarrassantes pour des groupes ou des individus. Certains lots de documents ont par la suite été publiés sur des sites dédiés à la fuite d'informations politiques controversées, dont *WikiLeaks*. Par ailleurs, le renseignement militaire russe (GRU) a aussi créé des devantures fictives pour la diffusion de ces documents. Ainsi, le site *DCLeaks* et la personnalité virtuelle de *Guccifer 2.0* était opérés par des agents du GRU.[266] Ces informations ont été diffusées à des moments politiquement sensibles. Ainsi, à la veille de la *Democratic National Convention*, *WikiLeaks* a publié plus de 20,000 courriels provenant du DNC. Cela a eu notamment comme conséquence la démission de Debbie Wasserman Schultz, présidente du DNC, pour avoir activement favorisé la candidature d'Hillary Clinton. Durant le mois précédent l'élection, *WikiLeaks* a graduellement publié les courriels subtilisés de John Podesta.[267]

e. Tentatives de recrutement ou de compromission

Des agents provenant de Russie ou se déclarant liés à des autorités russes ont entretenus des contacts avec des membres de la campagne électorale de Donald J. Trump.[268] Les relations d'affaires de Trump avec la Russie, soit le projet de construction d'une *Trump Tower* à Moscou, a été l'occasion pour des intermédiaires de tenter d'organiser une rencontre entre le candidat Trump et le président Poutine.[269] En janvier et

[265] J. B. Comey (2017), *Full Transcript and Video: James Comey's Testimony on Capitol Hill*, The New York Times, https://www.nytimes.com/2017/06/08/us/politics/senate-hearing-transcript.html
[266] R. S. Mueller III (2019), *Report on the investigation into Russian interference in the 2016 Presidential election Volume I of II*, United States Department of Justice, p.4, https://www.justsecurity.org/wp-content/uploads/2019/04/Muellller-Report-Redacted-Vol-I-Released-04.18.2019-Word-Searchable.-Reduced-Size.pdf
[267] CNN (2019), *2016 Presidential Campaign Hacking Fast Facts*, CNN Library, https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html
[268] R. S. Mueller III (2019), *Report on the investigation into Russian interference in the 2016 Presidential election Volume I of II*, United States Department of Justice, p.66, https://www.justsecurity.org/wp-content/uploads/2019/04/Muellller-Report-Redacted-Vol-I-Released-04.18.2019-Word-Searchable.-Reduced-Size.pdf
[269] *Ibid*, p.69 à 80.

en mars 2016, Trump a refusé à deux reprises des invitations à participer au Forum Économique International de St. Petersburg, dont une invitation provenait directement d'un vice-premier ministre du cabinet russe.[270] De plus, un aide présidentiel russe a approché, par une tierce personne américaine, deux candidats républicains aux élections présidentielles, dont Donald Trump, pour des invitations au *Roscongress* (l'organisateur du Forum Économique de St. Petersburg).

D'autres individus disant avoir des contacts hauts placés en Russie ont aussi approché des membres de la campagne de Trump (George Papadopoulos en avril 2016[271] et Donald Trump jr. en juin 2016[272]) en affirmant avoir des informations salissantes (*dirt*) sur Hillary Clinton. Bien qu'aucune accusation criminelle de collusion n'ait été portée contre la campagne de Trump, ces exemples montrent que des tentatives de contacts ont été faites par des représentants officiels ou officieux du gouvernement de Moscou, incluant Vladimir Poutine, avec Trump et son équipe de campagne. Cela peut signifier une tentative de collaboration discrète entre l'administration russe et une éventuelle administration Trump ou une tentative de compromettre Trump et son entourage pour les placer dans une position domestique vulnérable.

[270] *Ibid*, p.79
[271] *Ibid*, p.81
[272] *Ibid*, p.110

G. L'élection présidentielle française de 2017

> For the Kremlin, the stakes are high in the French elections. (…) The run-up to the elections offers the Russian government a chance to either help usher a more sympathetic figure into power in Paris or to create enough chaos to keep France focused on its own problems for the near future. The country is already deeply divided, making it all the more vulnerable to Russian influence.[273]
>
> - Stratfor assessment

a. Appui du Kremlin au Front National

Le dernier tour des élections françaises de 2017 s'est joué entre les candidats Emmanuel Macron et Marine Le Pen. Le Kremlin a développé une préférence pour Marine Le Pen à la suite de la défaite du candidat François Fillon, embrouillé dans un scandale d'emplois fictifs. Ce dernier était en faveur d'un rapprochement avec la Russie.[274] Madame Le Pen possède de nombreuses caractéristiques qui font d'elle une partenaire naturelle pour le Kremlin. Elle a mise de l'avant l'idée d'un *Frexit* (une sortie de la France de l'Union Européenne) et d'une sortie de l'OTAN. Elle tient un discours négatif envers l'immigration, nationaliste et favorise un leadership fort, conservateur tout en souhaitant de meilleures relations avec la Russie.[275] Contrairement à elle, Emmanuel Macron représentait le candidat du renforcement de l'ordre international libéral et d'une intégration plus poussée avec l'Union Européenne.

Vladimir Poutine a officiellement reçu Mme Le Pen au Kremlin à moins d'un mois du premier tour de l'élection présidentielle. Lors de cette rencontre, Poutine déclarait que Mme Le Pen « représente un spectre politique en Europe qui croît rapidement »[276]. En

---

[273] Stratfor (2017), *Russia Campaigns for the French Presidency*, Stratfor Worldview, https://worldview.stratfor.com/article/russia-campaigns-french-presidency

[274] E. Walkowiak et L. Holmes (2017), *Russia's meddling in the French elections: How and why?*, Election Watch, University of Melbourne, https://electionwatch.unimelb.edu.au/articles/russias-meddling-in-the-french-elections-how-and-why

[275] *Ibid*.

[276] I. Mandraud (2017), *À Moscou, Vladimir Poutine adoube Marine Le Pen*, Le Monde, https://www.lemonde.fr/election-presidentielle-2017/article/2017/03/24/marine-le-pen-recue-par-vladimir-poutine-a-moscou_5100247_4854003.html

2014, le Front National, le parti de Mme Le Pen, recevait un prêt de 9 millions d'euros (€) d'une banque de Moscou, la *First Czech Russian Bank*. Des analystes ont accusé Mme Le Pen d'avoir obtenu ce prêt en échange de son appui politique à l'annexion de la Crimée par la Russie.[277] À l'époque, plusieurs partis de l'extrême droite européenne apportait leur caution aux résultats du référendum de Crimée, dont le Front National.[278] Toutefois, en 2015, des messages textes de Timur Prokopenko, responsable des médias au sein de l'administration présidentielle russe, sont volées par des pirates informatiques et remis à la presse. Dans ceux-ci, des indices indiquent que cet appui aurait pu être négocié en échange d'un financement. Un interlocuteur écrit ainsi à Prokopenko que « le Front national prendra officiellement position sur la Crimée »[279]. Ils discutent par la suite de la question d'un financement. Dans un échange subséquent, suivant la prise de position publique du Front National, ils écrivent alors qu'il « faudra remercier les Français d'une manière ou d'une autre »[280]. En prévision des élections de 2017, le Front National demandait en 2016 un nouveau prêt de 27 millions d'euros (€) à des banques russes, à la suite du refus des institutions françaises de prêter à ce parti.[281]

Le Front National a officiellement un « accord de coopération » avec le Kremlin, comme de nombreux autres partis d'extrême-droite en Europe. « These cooperation agreements include plans for regular meetings and collaboration where suitable on economic, business and political projects. »[282]

---

[277] M. A. Orenstein (2015), *Putin's Western Allies Why Europe's Far Right Is on the Kremlin's Side*, Foreign Affairs, https://www.foreignaffairs.com/articles/russia-fsu/2014-03-25/putins-western-allies

[278] Le Monde (2015), *Financement du FN : des hackers russes dévoilent des échanges au Kremlin*, https://www.lemonde.fr/les-decodeurs/article/2015/04/02/fn-des-hackers-russes-devoilent-des-echanges-au-kremlin_4608660_4355770.html

[279] Le Monde (2015), *Financement du FN : des hackers russes dévoilent des échanges au Kremlin*, https://www.lemonde.fr/les-decodeurs/article/2015/04/02/fn-des-hackers-russes-devoilent-des-echanges-au-kremlin_4608660_4355770.html

[280] *Ibid.*

[281] C. Bremner (2016), *Le Pen's party asks Russia for €27m loan*, The Sunday Times, https://www.thetimes.co.uk/article/le-pens-party-asks-russia-for-euro27m-loan-kzxq8m7s30v

[282] U.S. Senate Committee on Foreign Relations (2018), *PUTIN'S ASYMMETRIC ASSAULT ON DEMOCRACY IN RUSSIA AND EUROPE: IMPLICATIONS FOR U.S. NATIONAL SECURITY*, United States Senate, p.50, https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

b. Propagande médiatique et désinformation dans les médias sociaux

La chaîne *Russia Today* (RT) a été très active dans sa couverture de la campagne électorale française. Entre le 5 février 2017 et le 17 avril 2017 (les élections du premier tour ayant eu lieu le 23 avril), 145 017 utilisateurs de Twitter ont été touchés par le contenu diffusé par RT.[283] Toutefois, la vaste majorité de ces utilisateurs n'ont interagi qu'une seule fois avec ce contenu. Seul 14 792 utilisateurs ont interagi deux fois ou plus avec ces publications, tandis que le nombre descend à 6006 pour 10 interactions ou plus.[284] Ainsi, les publications de RT ont atteint une très large audience durant cette période, mais seule une très petite audience semble s'être engagée sérieusement avec celles-ci. Parmi ces 6006 utilisateurs les plus actifs, les contenus publiés concernaient soit Emmanuel Macron sous un angle négatif ou traitaient sous un angle positif une des trois communautés les plus représentées dans ces tweets : l'Union Populaire République (UPR)[285], le parti La République (LR)[286] ou le Front National (FN). La communauté la plus active étant celle du FN.[287]

Une autre étude basée sur 842 000 tweets recueillis entre le 13 et le 19 mars 2017 montre un portrait plus élargi de la portion de fausses nouvelles dans l'environnement informationnel précédent les élections. La part de ce contenu caractérisé comme étant des fausses nouvelles est de 4.17%. En comparaison, la part de contenu publié par les médias russes officiels (Sputnik, RT, etc.) était de 2.45%. Ces deux sources d'information ont donc représenté ont faible pourcentage des nouvelles consommées par le public, considérant que 62.4% du contenu provenait soit des sites d'informations professionnels ou d'organismes politiques professionnels.[288] Parmi ces fausses nouvelles, de nombreuses fausses rumeurs

[283] N. Vanderbiest (2017), *Quelle est l'influence russe sur la campagne présidentielle française?* Reputatio Lab, p.2, https://www.les-crises.fr/wp-content/uploads/2018/09/1-reputatio-lab-20-04-2018.pdf
[284] *Ibid*, p.3.
[285] Parti politique français qui milite pour une sortie de l'Union Européenne.
[286] Parti dont le chef était alors François Fillon.
[287] *Ibid*, p.3-7.
[288] P. N. Howard, S. Bradshaw, B. Kollanyi et al. (2017), *Junk News and Bots during the French Presidential Election: What Are French Voters Sharing Over Twitter?*, DATA MEMO 2017.3, Project on Computational Propaganda, University of Oxford, p.4, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/04/What-Are-French-Voters-Sharing-Over-Twitter-v9.pdf

ont circulées concernant Emmanuel Macron, en passant d'une relation secrète avec sa belle-fille au fait qu'il se laverait les mains après avoir serrée celle des ouvriers.[289]

La part de ces fausses nouvelles directement attribuable à la désinformation russe est toutefois inconnue. Des groupes américains ou européens disséminent aussi des fausses nouvelles pour des raisons financières (publicités liées au nombre de clics) ou idéologique (extrême-droite, nationalisme, anti-immigration, etc.). Cependant, lors du scandale du #Macrongate[290], 5% des comptes de Twitter ayant publié avec cet *hashtag* ont représenté 40% des tweets.[291] Cette activité frénétique est indicatrice de l'action des *bots*, qui sont régulièrement utilisés par les Russes pour amplifier des informations avantageuses. Ceci est un donc indicateur de la présence d'activités russes parmi ces fausses nouvelles, bien qu'elle ne puisse pas être quantifiée avec précision.

c. Piratages informatiques

En février 2017, les représentants de la campagne d'Emmanuel Macron ont rapporté que des milliers d'attaques ont été effectuées sur leurs serveurs informatiques. Les employés ont aussi été victimes d'hameçonnages et cela a rendu les serveurs de la campagne accessibles à des acteurs externes.[292] Ultérieurement, Facebook a confirmé que des agents russes ont utilisé douze faux comptes pour entrer en contact avec des proches de Macron et tenter d'obtenir des renseignements.[293] Un proche de Macron affirmait alors :

---

[289] M. de Fournas (2017), *Présidentielle: 14 fake news qui circulent sur Emmanuel Macron*, 20 minutes France, https://www.20minutes.fr/high-tech/2058855-20170428-presidentielle-14-fake-news-circulent-emmanuel-macron

[290] Ce *hashtag* réfère au vol et à la fuite de 9 gigaoctet de données appartenant à la campagne d'Emmanuel Macron. Le paragraphe suivant apporte plus de précisions.

[291] K. Shaffer, C.E. Carey et B. Starling (2017), *Democracy Hacked: A Massive, Pro-Le Pen Disinformation Campaign Hits Twitter, 4chan, and the Mainstream Media*, Data for Democracy, paragraphe: Who's tweeting?, https://medium.com/data-for-democracy/democracy-hacked-a46c04d9e6d1

[292] S. Davis (2018), *RUSSIAN MEDDLING IN ELECTIONS AND REFERENDA IN THE ALLIANCE*, NATO Parliamentary Assembly, Science and Technology Committee (STC), p.8, https://www.nato-pa.int/document/2018-russian-meddling-elections-and-referenda-alliance-davis-report-181-stc-18-e-fin

[293] E. Brattberg et T. Maurer (2018), *RUSSIAN ELECTION INTERFERENCE: Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, p.9, https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf

> On essaie de rentrer informatiquement pour récupérer les données de nos 185,000 adhérents, pour avoir accès aux échanges de mails qui se font au sein de l'équipe ou alors pour avoir accès à des informations confidentielles sur la stratégie de campagne.[294]

Le 5 mai, deux jours avant le deuxième tour de l'élection, une vaste fuite de documents concernant la campagne d'Emmanuel Macron apparaît sur internet. On y retrouve des courriels de la campagne, des contrats, des documents de comptabilité et autres. Selon les responsables de la campagne de Macron, on retrouve aussi parmi ces fichiers, de nombreux faux documents visant à créer du doute et à embarrasser la campagne.[295]

Bien que, pour le chef de la cybersécurité du gouvernement français, les preuves étaient insuffisantes pour attribuer une origine précise à cette attaque, le directeur de la *National Security Agency* (NSA) américaine affirmait que les Russes étaient probablement à l'origine de cette attaque.[296] De son côté, la firme de sécurité privée *Trend Micro* attribuait plusieurs des tentatives d'hameçonnage au groupe *Fancy Bear*, considéré par le renseignement américain comme étant lié aux services de renseignement russes (GRU).[297] Le Secrétaire général du mouvement En Marche! a, pour sa part, clairement accusée la Russie de vouloir « déstabiliser la présidentielle en France »[298].

---

[294] M. Préel et J. Marot (2017), *Macron accuse Moscou d'ingérence au profit de Fillon et de Le Pen*, Le Devoir, https://www.ledevoir.com/monde/europe/491705/presidentielle-francaise-macron-accuse-moscou-d-ingerence-au-profit-de-fillon-et-de-le-pen

[295] S. Davis (2018), *RUSSIAN MEDDLING IN ELECTIONS AND REFERENDA IN THE ALLIANCE*, NATO Parliamentary Assembly, Science and Technology Committee (STC), p.8, https://www.nato-pa.int/document/2018-russian-meddling-elections-and-referenda-alliance-davis-report-181-stc-18-e-fin

[296] *Ibid.*

[297] E. Brattberg et T. Maurer (2018), *RUSSIAN ELECTION INTERFERENCE: Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, p.9, https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf

[298] R. Ferrand (2017), *Ne laissons pas la Russie déstabiliser la présidentielle en France !*, Le Monde, https://www.lemonde.fr/election-presidentielle-2017/article/2017/02/14/ne-laissons-pas-la-russie-destabiliser-la-presidentielle-en-france_5079213_4854003.html

H. L'élection fédérale allemande de 2017

> The German federal elections were significant mostly because of the apparent absence of Russian interference despite previous alleged disinformation campaigns and cyber attacks against German government targets. Besides the government's active preparations, high-level officials' clear warnings to Russia against interfering likely served as an added deterrent.[299]
>
> - Brattberg et Maurer

a. Collecte d'informations et cyberespionnage

En mai 2015, des pirates informatiques russes ont envoyé des courriels d'hameçonnage à des membres du gouvernement allemand. En cliquant sur un lien dans le courriel, des employés ont téléchargé un virus de type cheval de Troie. Les pirates ont visé le gouvernement durant un congé férié, alors que le département des technologies de l'information était fermé.[300] Cinq mille six cents ordinateurs et 12,000 utilisateurs ont été affectés, incluant 16 membres du parlement allemand (*Bundestag*) et le bureau de la chancelière Angela Merkel. En tout, 16 gigabits de données ont été volées dans ce qui était la plus grande cyberattaque de l'histoire du gouvernement allemand. Le renseignement allemand a attribué la responsabilité de cette attaque au groupe APT28 (*Fancy Bear*).[301] Des journalistes allemands du *Zeit* ont eu accès (avec autorisation) à un rapport classifié du renseignement allemand qui attribue explicitement la responsabilité d'autoriser ces opérations à l'administration présidentielle russe. Ainsi :

---

[299] E. Brattberg et T. Maurer (2018), *RUSSIAN ELECTION INTERFERENCE: Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, p.15, https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf

[300] S. Davis (2018), *RUSSIAN MEDDLING IN ELECTIONS AND REFERENDA IN THE ALLIANCE*, NATO Parliamentary Assembly, Science and Technology Committee (STC), p.8, https://www.nato-pa.int/document/2018-russian-meddling-elections-and-referenda-alliance-davis-report-181-stc-18-e-fin

[301] C. Stelzenmüller (2017), *The Impact of Russian Interference on Germany's 2017 Elections: Testimony before the U.S. Senate Select Committee on Intelligence*, Brookings Institution, p.7, https://www.intelligence.senate.gov/sites/default/files/documents/sfr-cstelzenmuller-062817b.pdf

> The BND[302] and BfV[303] presented a top secret report stating it "could be determined that present-day Russia centrally controls its influencing activities directed against the West." Cyberoperations like the one perpetrated against the Bundestag, which seek to "exert influence, and presumeably also to spread disinformation and propaganda on a grand scale," were likely "directly authorized by the presidential administration in the Kremlin and left up to the services to carry out." In other words: German intelligence is convinced Vladimir Putin is behind Fancy Bear. [304]

Le chef du renseignement intérieur allemande (BfV) a réitéré publiquement cette accusation quelques mois avant les élections présidentielles de 2017, tout en servant un avertissement implicite au Kremlin. En parlant de la cyberattaque de 2015 et de deux attaques subséquentes sur des fondations près de la coalition politique du gouvernement, il déclarait : « We recognize this as a campaign being directed from Russia. Our counterpart is trying to generate information that can be used for disinformation or for influencing operations. Whether they do it or not is a political decision ... that I assume will be made in the Kremlin. »[305]

Les informations acquises dans ces cyberattaques n'ont à ce jour jamais été révélées publiquement, contrairement à celles volées aux campagnes de Clinton et de Macron. Selon un rapport du Sénat américain, il est possible que ces informations n'aient pas été rendues publiques à cause des préoccupations du Kremlin liées à la réaction de la chancelière allemande, dont la réélection était très probable.[306]

b. Propagande médiatique

En Allemagne, la Russie dirige trois médias de langue allemande : *RT Deutsch*, *Sputnik Deutsch* et *NewsFront Deutsch*. Ce dernier prétend être indépendant, mais sa ligne

[302] Service de renseignement extérieur allemand
[303] Service de renseignement intérieur allemand
[304] P. Beuth, K. Biermann, M. Klingst et H. Stark (2017), *Cyberattack on the Bundestag: Merkel and the Fancy Bear*, Zeit Online, https://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia/komplettansicht
[305] A. Shalal (2017), *Germany challenges Russia over alleged cyberattacks*, Reuters, https://www.reuters.com/article/us-germany-security-cyber-russia/germany-challenges-russia-over-alleged-cyberattacks-idUSKBN1801CA
[306] U.S. Senate Committee on Foreign Relations (2018), *PUTIN'S ASYMMETRIC ASSAULT ON DEMOCRACY IN RUSSIA AND EUROPE: IMPLICATIONS FOR U.S. NATIONAL SECURITY*, United States Senate, p.130.

éditoriale suit pourtant celle du Kremlin. Un ancien employé prétend même qu'une large part de son budget provient des services secrets russes.[307] Ces trois médias sont toutefois des acteurs mineurs du paysage médiatique allemand. Sur Twitter, *RT* a 29,200 abonnés, *Sputnik* 14,700 et *NewsFront* 2,254. Par comparaison, les deux plus grands médias allemands, *Die Welt* et *Zeit Online,* ont respectivement 1,23 millions et 1,89 millions d'abonnés. Les médias russes font meilleures figures sur Facebook avec 270,000 abonnés pour *RT*, 181,000 pour *Sputnik* et 11,000 pour *NewsFront*, tandis que *Zeit Online* en a 773,000 et *Die Welt* 868,000.[308] Les médias russes ciblent trois groupes en Allemagne : la droite nationaliste, la gauche et les Allemands d'origine russe.[309]

Le parti politique *Alternativ fûr Deutschland* (*AfD*) est le plus proche de la Russie idéologiquement et personnellement. Certains politiciens de l'*AfD* ont des liens personnels avec la Russie, bien qu'aucun financement provenant de ces liens n'ait été démontré. Leur agenda politique rejoint bien souvent celui des nationalistes russes. L'*AfD* appuie par exemple l'annexion de la Crimée en affirmant qu'il s'agissait originellement d'un territoire appartenant à la Russie. En 2017, Frauke Petry, alors cheffe du parti, avait tenu une rencontre privée avec des représentants de haut niveau du gouvernement pour discuter de coopération.[310] La ligne éditoriale des médias russes présentait l'*AfD* avec un biais positif, alors que le reste des partis politiques et des institutions allemandes étaient dépeintes de façon négative. L'*AfD* était, selon cette couverture médiatique, un parti normal du paysage politique allemand maltraité par les médias dominants. Un grand espace était accordé à des

[307] C. Stelzenmüller (2017), *The Impact of Russian Interference on Germany's 2017 Elections: Testimony before the U.S. Senate Select Committee on Intelligence*, Brookings Institution, p.6, https://www.intelligence.senate.gov/sites/default/files/documents/sfr-cstelzenmuller-062817b.pdf
P. Beuth, M. Brost, P. Dausend et al. (2017), *War Without Blood,* Zeit Online, https://www.zeit.de/digital/internet/2017-02/bundestag-elections-fake-news-manipulation-russia-hacker-cyberwar/komplettansicht
[308] B. Nimmo (2017), *The Kremlin's Amplifiers in Germany The activists, bots, and trolls that boost Russian propaganda*, Digital Forensic Research Lab – Atlantic Council, https://medium.com/dfrlab/the-kremlins-amplifiers-in-germany-da62a836aa83
[309] A. Applebaum, P. Pomerantsev , M. Smith et C. Colliver (2017), *"MAKE GERMANY GREAT AGAIN" Kremlin, Alt-Right and International Influences in the 2017 German Elections*, Institute for Global Affairs, London School of Economics, p.5-6, http://www.lse.ac.uk/iga/assets/documents/arena/2017/Make-Germany-Great-Again-ENG-061217.pdf
[310] *Ibid*, p.10.

citations de l'*AfD* et à ses promesses électorales favorables aux intérêts russes, tel que la levée des sanctions commerciales sur la Russie.[311]

Le parti de gauche allemand (*Die Linke*)[312] tient des positions proches de Moscou concernant l'Ukraine, la Syrie, l'OTAN et les États-Unis. Les critiques des médias du Kremlin sur ces sujets rejoignent généralement cette audience. C'est ainsi que les accusations de fascisme contre les manifestants et les dirigeants ukrainiens, par exemple, trouvent écho dans les groupes antifascistes. Bien que ces groupes de gauche rejoignent parfois la trame narrative du Kremlin sur les médias sociaux, cela est moins fréquent que chez les groupes de la droite nationaliste. Par ailleurs, leurs intérêts et leurs sources d'informations sont plus diversifiées.[313]

Le groupe des Allemands d'origine russe (Russo-Allemands) est le plus influencé par les médias russes. Par ailleurs, il existe une forte association entre les médias russes, les Russo-Allemands et l'*AfD*. Ce parti est le premier et le seul à avoir développé une stratégie de campagne visant ce groupe d'électeurs avec des publications politiques en langue russe. Plusieurs candidats et activistes russo-allemands ont représenté ce parti. Alors que précédemment, les russo-allemands n'avaient été représentés qu'à une seule occasion dans les instances politiques allemandes, l'*AfD* a fait élire au *Bundestag* deux candidats de ce groupe. Une étude basée sur 1,500 comptes des réseaux sociaux a démontré que les Russo-Allemands se basent grandement sur les médias du Kremlin pour leurs sources d'information et sont particulièrement isolés des autres médias.[314] Durant la campagne électorale, des forums et des groupes sur les réseaux sociaux ont indiqué que cette communauté manifestait fréquemment des sentiments négatifs envers les réfugiés. Ces groupes virtuels révélaient un mélange de visions favorables à Poutine, de contenu anti-réfugié et dénigrant envers Merkel. Ces contenus circulaient sous forme de *meme*, de publications d'opinions ou d'articles provenant de *RT* ou *Sputnik*.[315] Même si les bons résultats électoraux de l'*AfD* à l'échelle de l'Allemagne ne sont pas directement

[311] *Ibid*, p.12.
[312] Il s'agit du parti ayant succédé au Parti socialiste unifié d'Allemagne. Ce parti a dirigé l'Allemagne de l'est durant plus de 50 ans.
[313] *Ibid*, p.14-15.
[314] *Ibid*, p.16-17-18.
[315] *Ibid*, p.18.

attribuables aux russo-allemands, il existe une forte corrélation entre une population russo-allemande élevée et des résultats électoraux élevés pour l'*AfD* dans ces régions.[316]

c. Désinformation

Un cas particulier de désinformation a eu un impact retentissant en Allemagne. En janvier 2016, une fille de 13 ans habitant à Berlin et provenant d'une famille d'immigrants russes du nom de Lisa a été portée disparue pendant 30 heures. Le réseau *First Russian TV* s'est emparé de la nouvelle, tout en ajoutant qu'elle avait été violée par des migrants d'origine arabe. Bien que la jeune fille ait originellement rapporté cette agression sexuelle, celle-ci s'est avérée fausse. Les policiers ont pu déterminer qu'elle avait plutôt passé la nuit avec une amie. Toutefois, la nouvelle a rapidement fait le tour de la Russie. *RT* et *Sputnik* l'ont reprise pour la diffuser en Allemagne, tout en conservant l'histoire de la fausse agression sexuelle. Les réseaux sociaux ont continué de propager cette information, puis des groupes russo-allemands et de néonazis ont organisé des manifestations. Ces mêmes médias russes ont alors fait des reportages sur ces manifestations. Cela a été porté à l'attention des médias dominants d'Allemagne qui ont répandu l'information à un plus vaste public.[317] Le ministre des Affaires étrangères de Russie, Sergei Lavrov, y est même allé de deux commentaires publics, dont une déclaration selon laquelle : « The accusation that investigators are covering something up does not become more correct, simply by continually repeating it ».[318] Cette affirmation faisait allusion à des théories du complot populaires sur internet selon lesquelles les autorités allemandes tentaient de cacher des faits embarrassants dans cette histoire. Ainsi, ce cas montre comment les méthodes de désinformation russes fonctionnent pour amplifier une fausse nouvelle et créer de la discorde concernant des enjeux controversés et sensibles. Cette fausse histoire jouait sur la peur des migrants, qui est un thème dominant de la narration russe. Elle visait à saper la

[316] *Ibid*, p.19.

[317] S. Meister (2016), *The "Lisa case": Germany as a target of Russian disinformation*, NATO Review magazine, https://www.nato.int/docu/review/2016/also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm

[318] D. McGuinness (2016), *Russia steps into Berlin 'rape' storm claiming German cover-up*, BBC News, https://www.bbc.com/news/blogs-eu-35413134

crédibilité du gouvernement auprès de sa population, alors que la politique d'ouverture et d'accueil des migrants était directement attribuable à la chancelière Merkel.[319]

D'une façon semblable, des *bots* automatisés ou partiellement contrôlés par des humains ont tenté d'amplifier la rhétorique du Kremlin avant et pendant la campagne électorale allemande.[320] Ces *bots* partageaient automatiquement les articles de *RT*, *Sputnik* et *NewsFront*. Ainsi, une étude de 2,460 comptes, déterminés comme étant pro-Kremlin par un algorithme, a trouvé que 60% d'entre eux étaient des *bots*. Ce réseau de comptes automatisés était actif durant la campagne électorale.[321] Il partageait, entre autres, répétitivement du contenu pro-*AfD* et anti-Merkel. Il a notamment amplifié les prétentions de fraudes électorales par l'extrême-droite. Ce réseau peut être associé à la Russie dû à la langue d'interface des comptes[322], qui était le russe. Cependant il est impossible de savoir exactement qui pilotait ceux-ci. L'utilisation variée de ce réseau de *bots* servant parfois à promouvoir des campagnes commerciales, nuire à un opposant politique (Alexeï Navalny) en Russie ou créer de la visibilité à un politicien de Vladivostok indique qu'il s'agirait d'un *bot* de location. Ceci signifie que ce réseau peut être loué par des clients pour amplifier le message de leur choix.[323] L'utilisation de ces *bots* peut servir à améliorer le rang des articles sur les engins de recherche et en augmenter la visibilité lors d'une recherche sur le sujet.[324]

---

[319] U.S. Senate Committee on Foreign Relations (2018), *PUTIN'S ASYMMETRIC ASSAULT ON DEMOCRACY IN RUSSIA AND EUROPE: IMPLICATIONS FOR U.S. NATIONAL SECURITY*, United States Senate, p.129, https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

[320] C. Stelzenmüller (2017), *The Impact of Russian Interference on Germany's 2017 Elections: Testimony before the U.S. Senate Select Committee on Intelligence*, Brookings Institution, p.6, https://www.intelligence.senate.gov/sites/default/files/documents/sfr-cstelzenmuller-062817b.pdf

[321] A. Applebaum, P. Pomerantsev , M. Smith et C. Colliver (2017), *"MAKE GERMANY GREAT AGAIN" Kremlin, Alt-Right and International Influences in the 2017 German Elections*, Institute for Global Affairs, London School of Economics, p.19, http://www.lse.ac.uk/iga/assets/documents/arena/2017/Make-Germany-Great-Again-ENG-061217.pdf

[322] La langue d'interface signifie que, pour l'utilisateur du compte, l'interface apparaît en russe sur son écran. Par contre, les publications peuvent être en anglais, en allemand ou dans n'importe quelle langue.

[323] B. Nimmo (2017), *#ElectionWatch: Russian Botnet Boosts German Far-Right Posts*, Digital Forensic Research Lab – Atlantic Council, paragraphe: Conclusion, https://medium.com/dfrlab/german-election-russian-botnet-boosts-far-right-posts-45f170bc2321

[324] D. Stukal, S. Sanovich, R. Bonneau et J. A. Tucker (2017). *Detecting Bots on Russian Political Twitter*. Big Data, 5(4), pp.310-324, https://www.liebertpub.com/doi/10.1089/big.2017.0038

VII. Analyse de la stratégie – cadre conceptuel

> Man possesses the ability to construct languages capable of expressing every sense, without having any idea how each word has meaning or what its meaning is -just as people speak without knowing how the individual sounds are produced.
>
> Everyday language is a part of the human organism and is no less complicated than it. It is not humanly possible to gather immediately from it what the logic of language is.
>
> Language disguises thought. So much so, that from the outward form of the clothing it is impossible to infer the form of the thought beneath it, because the outward form of the clothing is not designed to reveal the form of the body, but for entirely different purposes.
>
> The tacit conventions on which the understanding of everyday language depends are enormously complicated.[325]
>
> - Ludwig Wittgenstein

a. Processus stratégique

Afin de comprendre la stratégie russe, deux choses importantes ont jusqu'à présent été accomplies. Premièrement, une liste des méthodes a été donnée par la revue documentaire. Deuxièmement, une compréhension de l'utilisation de ces méthodes a été acquise grâce à l'étude de cas. Ces éléments peuvent maintenant être intégrés dans une conceptualisation du processus stratégique.

Le cadre théorique permettra de classifier ces méthodes en fonction de la forme de puissance utilisée afin d'en offrir une compréhension d'ensemble. Cette classification fera ressortir les stratégies possibles. Par la suite, le processus stratégique de déploiement de ces opérations sera conceptualisé selon les niveaux d'intensité des attaques informationnelles; le traitement de la donnée informationnelle; et le cycle opérationnel. Ces trois modèles rendent compte de la pensée stratégique se dissimulant en arrière-plan. Cette logique opérationnelle reflète la stratégie de contrôle russe camouflée au citoyen moyen dans son usage quotidien de l'information.

[325] Wittgenstein (1921), *Tractatus logico-philosophicus*, proposition 4.002, Routledge, 2e édition, 2001, p.22.

b. Classification des méthodes en fonction de leur environnement

Le cadre théorique de Nye permettra de classifier les méthodes des opérations d'information russes. Chacune des cases du tableau constitue un environnement opérationnel ayant ses stratégies particulières. En identifiant les stratégies possibles pour chaque environnement et en recensant celles utilisées par Moscou, il sera possible d'éclairer la structure de leurs opérations. Les stratégies identifiées permettront dans une prochaine étape de modéliser la structure et le cycle des opérations d'information

- Le tableau #1 catégorise les méthodes selon le type d'instruments (informationnels ou physiques) en fonction de leur environnement d'utilisation (interne ou externe au cyberespace).

MÉTHODES DES OPÉRATIONS D'INFORMATION RUSSES		
	INTRA-CYBERESPACE	EXTRA-CYBERESPACE
INSTRUMENTS INFORMATIONNELS	*Hard* : DDoS, fausses nouvelles (internet), hameçonnage pour voler des informations, trolls, bots, manipulation d'agents, espionnage *Soft* : fuite d'informations embarrassantes, propagande médiatique (internet), diplomatie publique (internet), recrutement d'agents d'influence	*Hard* : fausses nouvelles (télévisuelles) *Soft* : diplomatie publique, propagande médiatique (télévisuelle)
INSTRUMENTS PHYSIQUES	*Hard* : prise de contrôle ou destruction des réseaux de communication (internet) *Soft* : -	*Hard* : prise de contrôle ou destruction des réseaux de communication (autres qu'internet), assassinats de journalistes ou d'opposants, corruption, espionnage *Soft* : proximité idéologique et soutien financier à des partis politiques et des ONG, manifestations nationalistes

Instruments informationnels dans le cyberespace

Cet univers est un monde de pure information. Le seul moyen d'y agir est par le transfert d'informations. Lorsque les acteurs présentent ouvertement leurs actions ou leurs informations, il s'agit de *soft power.* Toutefois, lorsque les acteurs mentent volontairement ou contraignent par la force les informations des autres acteurs, alors s'agit de *hard power*. Quatre catégories d'actions sont possibles dans cet univers. Les acteurs peuvent :

1. Bloquer la diffusion des informations d'un adversaire
2. Voler les informations d'un autre acteur
3. Recruter ou manipuler des acteurs
4. Partager des informations en appui ou en opposition à des opinions.

L'ensemble de ces stratégies sont utilisées par la Russie, à la fois sous forme de *soft* et de *hard power*.

Instruments informationnels hors du cyberespace

Cet univers permet d'agir sur le monde informationnel à partir de l'extérieur du cyberespace. De la même façon que dans le cyberespace, l'information y est une forme de *soft power* lorsque l'acteur s'identifie pour présenter son point de vue et partage ouvertement ses informations. À l'opposé, le *hard power* correspond à un partage d'informations volontairement fausses. Deux stratégies sont possibles :

1. Effectuer des attaques informatiques contre la structure physique de support des espaces informationnels. Ces attaques informatiques peuvent viser des centrales énergétiques, des réseaux de serveurs ou autres infrastructures de support reliées à internet ou un serveur informatique.[326]
2. Contrôler les technologies précédentes de l'information : la télévision, la radio et les journaux papiers. Cette stratégie est assimilable à la propagande du 20^{e} siècle. Les

[326] Ce type d'action n'est pas commun dans les opérations d'information en temps de paix. Il est plus probable durant les opérations d'information en temps de guerre.

acteurs peuvent acheter ou fonder des médiums dans les pays adverses pour y propager un message favorable à leurs intérêts ou défavorable aux intérêts adverses.

Seule la deuxième stratégie a été utilisée par la Russie, à la fois sous forme de *soft* et de *hard power*.

Instruments physiques pour le cyberespace

Cet univers permet un contrôle légal du cyberespace par les États, de même qu'un contrôle technologique et économique par les grandes entreprises. De plus, les États ou les acteurs non-étatiques peuvent influencer les comportements par la distribution ou l'interdiction d'instruments physiques nécessaires pour accéder au cyberespace. Le *hard power* s'y exerce par la contrainte associée à l'interdiction d'accéder à certains outils technologiques. À l'opposé, le *soft power* fournit à des acteurs les moyens technologiques physiques pour exercer une influence d'attraction. Deux stratégies sont possibles :

1. Établir et appliquer des lois, règlements ou normes contre certains discours ou usages du cyberespace.[327]
2. Interdire ou distribuer le matériel physique nécessaire pour accéder ou diffuser certains contenus dans le cyberespace.[328]

Seule l'interdiction par la prise de contrôle ou la destruction du matériel physique est utilisée par Moscou et spécifiquement dans un contexte de guerre hybride. Ces stratégies sont plus pertinentes pour un usage intérieur.

[327] Les États ont cette capacité presqu'exclusivement à l'intérieur de leurs frontières. Ce qui fait que la Russie ne peut pas appliquer cette stratégie dans leurs opérations d'information à l'étranger (même si elle l'applique sur la scène domestique). Toutefois ce principe tend à changer avec la diffusion de plateformes d'informations à l'étranger, mais contrôlées de l'intérieur d'un État. Par exemple, WeChat est une plateforme grandement utilisée par les citoyens chinois des pays occidentaux, mais dont le contenu est fortement régulé par le Parti communiste chinois.

[328] Par exemple, un routeur VPN est un système permettant notamment de contourner le *firewall* de la Chine et d'accéder au contenu occidental interdit. Des organisations peuvent aussi, comme en Corée du Nord, distribuer des clés USB contenant du contenu informationnel interdit par le régime.

Instruments physiques hors du cyberespace

Cet univers permet de contrôler l'environnement informationnel à partir du monde physique. Les acteurs peuvent agir sur les structures ou les individus qui régulent le flot d'informations. Le *hard power* consiste à contraindre physiquement, économiquement ou par la tromperie des acteurs ou des infrastructures, tandis que le *soft power* vise à attirer les acteurs partageant une proximité idéologique ou des intérêts communs vers l'accomplissement de certaines actions. Quatre stratégies sont possibles :

1. Contrôler ou détruire les réseaux de communication.
2. Menacer, assassiner, corrompre ou espionner des individus.[329]
3. Appuyer ou développer des liens de collaboration avec des partis politiques ou des acteurs sociaux (ONG) partageant une idéologie ou des intérêts communs.
4. Organiser des manifestations en faveur de nos intérêts ou contre les intérêts adverses.

Toutes ces stratégies sont utilisées par la Russie, sous forme de *soft* et de *hard power*.

Analyse de la première classification théorique

L'application de cet outil théorique permet de tirer quelques conclusions partielles. D'abord, il y a une continuité entre la forme que prenait la propagande dans l'espace informationnel hors du cyberespace et les opérations d'information modernes dans le cyberespace. Lorsque la population fait encore majoritairement usage des médias télévisuels, radiophoniques et des journaux papiers, Moscou déploie ses organismes de propagande traditionnels pour occuper ce territoire. Cet environnement est particulièrement applicable aux pays moins développés de l'ancienne Union Soviétique (États baltes et Ukraine), ainsi qu'aux russophones de l'ancienne Allemagne de l'est.

Avec le développement du cyberespace, les opérations d'informations se sont graduellement déplacées pour occuper ce nouvel environnement. Une autre constatation est que les stratégies de contrôle et d'influence dans cet environnement se sont multipliées.

[329] Sur la scène domestique les options de l'État sont plus larges, tel que l'emprisonnement ou l'imposition d'amendes aux individus récalcitrants.

En effet, l'environnement informationnel du cyberespace offre aux acteurs plus d'options de contrôle et d'influence que l'environnement informationnel de la propagande du 20e siècle. En particulier, les méthodes de *hard power* pour contrôler et manipuler l'information se sont grandement améliorées.

Troisièmement, l'État peut difficilement réguler le flot d'informations hors de ses frontières. Toutefois, les instruments technologiques et législatifs du contrôle de l'information se sont développés à l'intérieur des États autoritaires. Par ailleurs, les instruments de contrôle physiques tendent à disparaître alors que l'information transite de moins en moins par un support physique.[330] L'établissement des normes et des standards de l'internet est une autre dimension de la guerre de l'information se jouant dans les institutions internationales. Ces aspects ne font toutefois pas partie des opérations d'information à proprement parler.

Finalement, les instruments physiques s'emploient conjointement avec des opérations d'information. Le phénomène de la guerre hybride implique un contrôle sur le territoire géographique, sur les infrastructures de communication de même que sur l'environnement informationnel, particulièrement dans le cyberespace. Le contrôle de l'information dans des sociétés vulnérables peut passer par le contrôle des individus associés à la transmission d'informations. Les assassinats, la corruption et l'espionnage peuvent soumettre les personnes transmettant des informations défavorables. Au contraire, le Kremlin peut soutenir les acteurs politiques et les organisations de la société civile favorables à ses intérêts.

En résumé, il est possible de faire usage de quatre grandes stratégies :

c. Dénier la transmission d'informations
d. Voler de l'information
e. Manipuler par l'information
f. Amplifier l'information.

Les opérations d'informations modernes de la Russie emploient ces quatre stratégies.

[330] L'usage des CD, DVD, clés USB ou autres supports physiques est de plus en plus remplacée par l'infonuagique, le stockage et le téléchargement en ligne.

c. Classification des méthodes en fonction des aspects de la puissance

Nye définissait trois aspects à la puissance dans son cadre théorique. Un acteur peut influencer un autre acteur en (1) l'incitant à agir de façon contraire à sa volonté; (2) limitant ses choix en rendant certaines stratégies inutilisables; (3) façonnant ses préférences. Une classification des méthodes selon ce cadre permet de constater que Moscou fait principalement usage du premier et du troisième aspect dans ses opérations d'information, tandis que le deuxième aspect est utilisé dans un cadre de guerre hybride.

- Le tableau #2 classifie les méthodes en fonction des trois aspects de la puissance.

PREMIER ASPECT A INCITANT B À FAIRE CE QUE B N'AURAIT PAS INITIALEMENT FAIT
Hard : Hameçonnage, trolls, bots, manipulation d'agents, espionnage, corruption Soft : manifestations nationalistes, recrutement d'agents d'influence, proximité idéologique et soutien financier à des partis politiques et des ONG
DEUXIÈME ASPECT A LIMITANT LES CHOIX DE B EN EXCLUANT LES STRATÉGIES DE B
Hard : prise de contrôle ou destruction des réseaux physiques de communication, DDoS, assassinats Soft : -
TROISIÈME ASPECT A FAÇONNANT LES PRÉFÉRENCES DE B DE TELLE SORTE QUE CERTAINES STRATÉGIES NE SONT MÊME PAS CONSIDÉRÉES
Hard : fausses nouvelles (internet et télévision) Soft : fuite d'informations embarrassantes, propagande médiatique (internet et télévision), diplomatie publique

Conformément aux conclusions sur les instruments physiques dans le cyberespace, Moscou peut plus difficilement limiter les choix d'un acteur B hors de ses frontières. Ce deuxième aspect de la puissance est principalement applicable à l'intérieur des frontières d'un État. Ce dernier peut exclure les stratégies de sa population par l'application de lois. Sur la scène internationale, cet aspect peut se manifester par les normes et standards internationaux. Il n'est donc pas envisageable qu'une opération d'information puisse limiter les choix d'individus hors de ses frontières en excluant à grande échelle certaines idées ou stratégies. C'est plutôt lorsqu'une pure opération d'information échoue, que l'intervention d'une stratégie hybride impliquant le pouvoir militaire est nécessaire pour exclure certains choix à un acteur. C'est ainsi que les choix de Kiev ont été limités par la saisie militaire de la Crimée et l'insurrection au Donbass. À plus petite échelle, la peur d'être assassiné peut limiter certains choix, tandis que les attaques DDoS bloquent temporairement accès à de l'information.

Les opérations d'information permettent principalement d'inciter et de façonner les préférences des acteurs. Ils peuvent être influencés par la contrainte (*hard power*) ou par l'attirance (*soft power)*. Moscou fait usage des deux stratégies en déniant, volant, manipulant et amplifiant de l'information, de même qu'en regroupant des agents intéressés autour de son influence. La diffusion d'informations vise ultimement à façonner les préférences des individus, conformément au concept de contrôle réflexif. La majorité de ces messages sont une propagande orientant les croyances par le *soft power* en présentant une opinion spécifique d'événements communs. En revanche, certains de ces messages sont de la désinformation visant à tromper délibérément par des mensonges une frange plus naïve de la population. Les théories du complot entrent dans cette dernière catégorie.

Au final, le cadre théorique permet de définir globalement les grandes stratégies propres aux opérations d'informations russes. Il ne permet pas d'offrir les détails nécessaires à une compréhension pointue, mais il oriente l'analyse sur trois points majeurs:

1. L'apparition de nouvelles stratégies de contrainte et de manipulation de l'information dans le cyberespace.
2. La coordination d'instruments physiques et informationnels d'influence.
3. Les stratégies d'incitation et de façonnement des préférences.

d. Occurrence des méthodes dans les opérations étudiées

Le tableau ci-dessous montre une vue synthétique des méthodes ayant été utilisées dans les opérations d'information étudiées. Une occurrence positive (✓) est indiquée lorsque les données analysées ont permis de démontrer une présence certaine ou très probable de l'État russe derrière les activités identifiées.

- Le tableau #3 recense les méthodes employées dans les opérations étudiées.

Opérations → ↓ Méthodes	Baltes	Géorgie	Ukraine	Suède	Royaume-Uni	États-Unis	France	Allemagne	*Total*
DDoS	✓	✓	✓	✓					4
Fausses nouvelles			✓	✓	✓	✓	✓	✓	6
Hameçonnage			✓			✓	✓	✓	3
Trolls			✓		✓	✓			3
Bots			✓	✓	✓	✓	✓	✓	6
Manipulation		✓				✓			2
Fuite d'info. compromettantes						✓	✓		2
Propagande	✓	✓	✓	✓	✓	✓	✓	✓	7
Diplomatie publique	✓	✓						✓	3
Contrôle des réseaux physiques		✓	✓						2
Assassinats			✓						1
Corruption			✓						1
Espionnage			✓			✓			2
Soutien - parti politique ou ONG	✓	✓	✓		✓		✓	✓	6
Manifestations	✓					✓			2

e. Niveaux d'intensité des opérations d'information

Les opérations d'information évoluent selon des niveaux d'intensité. Les ressources et l'agressivité des actions croissent en fonction de l'importance pour le Kremlin d'augmenter son contrôle de la sphère informationnelle. Quatre niveaux d'intensité ont été recensés, en correspondance avec la fréquence d'occurrence des méthodes et le niveau d'ingérence propre à chaque méthode.

A. Dans l'ensemble de l'étude de cas, la propagande médiatique de *RT*, *Sputnik* ou des autres chaînes d'information russes était présente. Des plateformes médiatiques suivant la ligne éditoriale du Kremlin sont un des fondements de ces opérations. Elle atteint à la fois les populations russophones des pays ciblés, de même que les populations locales dans les marges du spectre politique. La diplomatie publique des autorités du Kremlin intervient particulièrement lorsque des populations russophones sont concernées. Dans les pays baltes, en Géorgie et en Allemagne, les autorités du Kremlin présentaient les gouvernements de ces pays comme opposés aux intérêts des populations russophones locales.

Ces formes de propagande sont en continuité avec la propagande soviétique, qui passait alors par les médiums télévisuels, radiophoniques ou papiers. La nouvelle propagande se déployant maintenant principalement sur internet amène une distinction importante. Le cyberespace permet une plus grande manipulation de l'information. De plus, l'interconnexion globalisée entre les individus et les plateformes internet augmente la portée de pénétration du contenu. Il y a donc une différence qualitative et quantitative par rapport à la propagande de l'ère soviétique.

Le rapprochement du Kremlin avec des partis politiques, en particulier ceux très à droite en Europe, est aussi une constante du paysage politique. Toutefois, Moscou ne trouve pas toujours une oreille attentive. Ainsi, malgré des tentatives de contact, Donald Trump a refusé d'entretenir des liens avec le Kremlin durant sa campagne électorale.

B. À partir de ce bruit de fond, plusieurs actions peuvent être portées. En premier lieu, les fausses nouvelles, les *bots* et les *trolls*, permettent d'intégrer du faux contenu plus

controversé ou scandaleux, et amplifier la propagande pour accentuer les tensions et les divisions sur des enjeux sensibles. Ces techniques apparaissent à grande échelle aux environs de 2014 en Ukraine, en Suède et aux États-Unis. Cela correspond aux découvertes du renseignement américain selon lequel l'*IRA* a débuté ses activités en 2013-2014. Les premiers comptes Twitter pour l'opération en Amérique ayant été créés en 2013 et les activités s'étant amplifiées et propagées aux autres plateformes à partir de 2014.

La désinformation et les *bots* sont maintenant une constante de ce nouvel environnement informationnel. Qu'elles soient propagées par les médias officiels ou par l'*IRA*, les actualités quotidiennes sont mélangées à des points de vue biaisés et de fausses informations. Elles sont par la suite amplifiées par des réseaux de bots, principalement à des moments clés d'un événement politique. Les *trolls* sont plus difficiles à détecter. Étant de véritables faux utilisateurs des réseaux sociaux, leurs opinions controversées se mélangent avec celles des autres utilisateurs. Ils sont toutefois fréquemment présents, en particulier lors des opérations majeures comme en Ukraine ou aux États-Unis.

C. Un niveau supérieur d'une opération d'information est représenté par des techniques d'hameçonnage et des fuites d'informations embarrassantes. Cette technique a été particulièrement remarquée aux États-Unis, en France et en Allemagne. À l'exception de l'Allemagne, les informations volées ont été dévoilées sur des sites internet à des moments clés des élections. Lorsque la propagation de fausses nouvelles, d'opinions controversées par les *trolls* et l'amplification de ces contenus par les *bots* atteint un seuil critique, certaines franges de la population peuvent être incitées à poser des actes physiques comme des manifestations.

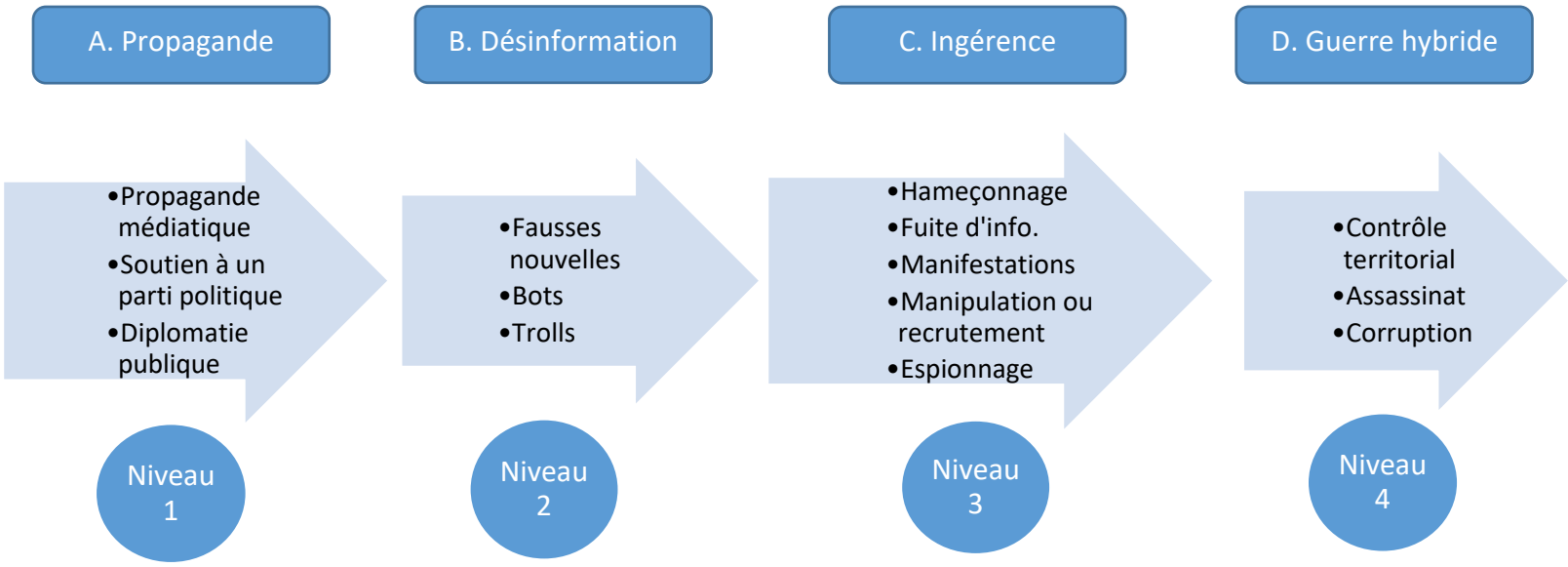
La situation socio-politique doit toutefois être suffisamment tendue et l'implication étrangère assez élevée pour que ces individus fictifs réussissent à mener la population à des démonstrations physiques suivant l'influence extérieure. C'était le cas aux États-Unis, alors que l'opération russe y déployait des ressources considérables. À ce stade, la manipulation ou le recrutement d'individus est envisageable. Des individus ciblés peuvent propager le message encore plus profondément dans la population ou des décideurs politiques peuvent être incités à poser des gestes défavorables (Géorgie). Ces actions sont

soutenues par de l'espionnage physique ou informatique afin d'identifier les vulnérabilités à cibler.

D. Le dernier niveau d'intensité des opérations d'information implique une intervention agressive dans le pays ciblé. C'est à ce stade que les opérations d'information se transforment en guerre hybride. L'armée peut prendre le contrôle du territoire physique, incluant les réseaux de communication. Les services de renseignement peuvent effectuer des assassinats, de la corruption ou toute autre forme de subversion.

Les attaques DDoS représentent un type particulier d'actions. Elles sont survenues lors d'opérations de basse intensité (pays baltes, Suède) et d'intensité élevée (Géorgie, Ukraine). Elles sont associées à des tentatives d'intimidation ou de blocage des communications et se retrouvent à plusieurs niveaux dans le spectre des conflits.

- Le tableau #4 représente la progression d'intensité des opérations d'information avec les techniques associées.



f. Les quatre stratégies en fonction des trois aspects de la puissance

Ces niveaux d'intensité correspondent à quatre stratégies. L'utilisation d'une stratégie de niveau supérieur sert à augmenter la pression psychologique sur la société visée. Les stratégies reflètent les trois aspects de la puissance du cadre théorique.

1. Le premier niveau vise à façonner les préférences de la société d'accueil par la présentation du choix désiré. Par la voie de ses médias, de ses interventions publiques et de ses associations politiques, le Kremlin invite la population et façonne doucement certaines préférences.
2. Si la population n'adopte pas les préférences du Kremlin (ou s'il était prévu dès le départ qu'elle ne le ferait pas), des techniques d'incitation peuvent être déployées. L'opinion désirée peut être manipulée et amplifiée par des *trolls* et des *bots*. L'hameçonnage peut conduire à des révélations embarrassantes, façonnant plus profondément les préférences individuelles. De fausses personnalités virtuelles peuvent inciter à des manifestations ou des opinions conforment à la direction souhaitée. Les stratégies du deuxième et troisième niveau incitent à la conformité avec la préférence.
3. Dans l'éventualité où la préférence désirée n'est toujours pas adoptée, alors le Kremlin peut parfois intervenir pour exclure au sujet certains choix grâce à des méthodes de *hard power* comme les interventions militaires, les assassinats ou la corruption.

g. Structure conceptuelle des techniques informationnelles

Les données informationnelles ont une structure de déploiement à l'image de l'opération elle-même. La donnée de base est développée par le réseau médiatique russe et les interventions publiques des autorités russes. À celle-ci s'ajoute les fausses nouvelles, qui sont souvent créées par le réseau de désinformation associé aux « fermes de trolls ». Ces données présentent de façon binaire les options du choix. En simplifiant les thèmes, ils se réduisent en une mauvaise option, le libéralisme universaliste et démocratique occidental, et une bonne option, les valeurs traditionnelles, conservatrices, relativistes et autoritaires de la Russie.

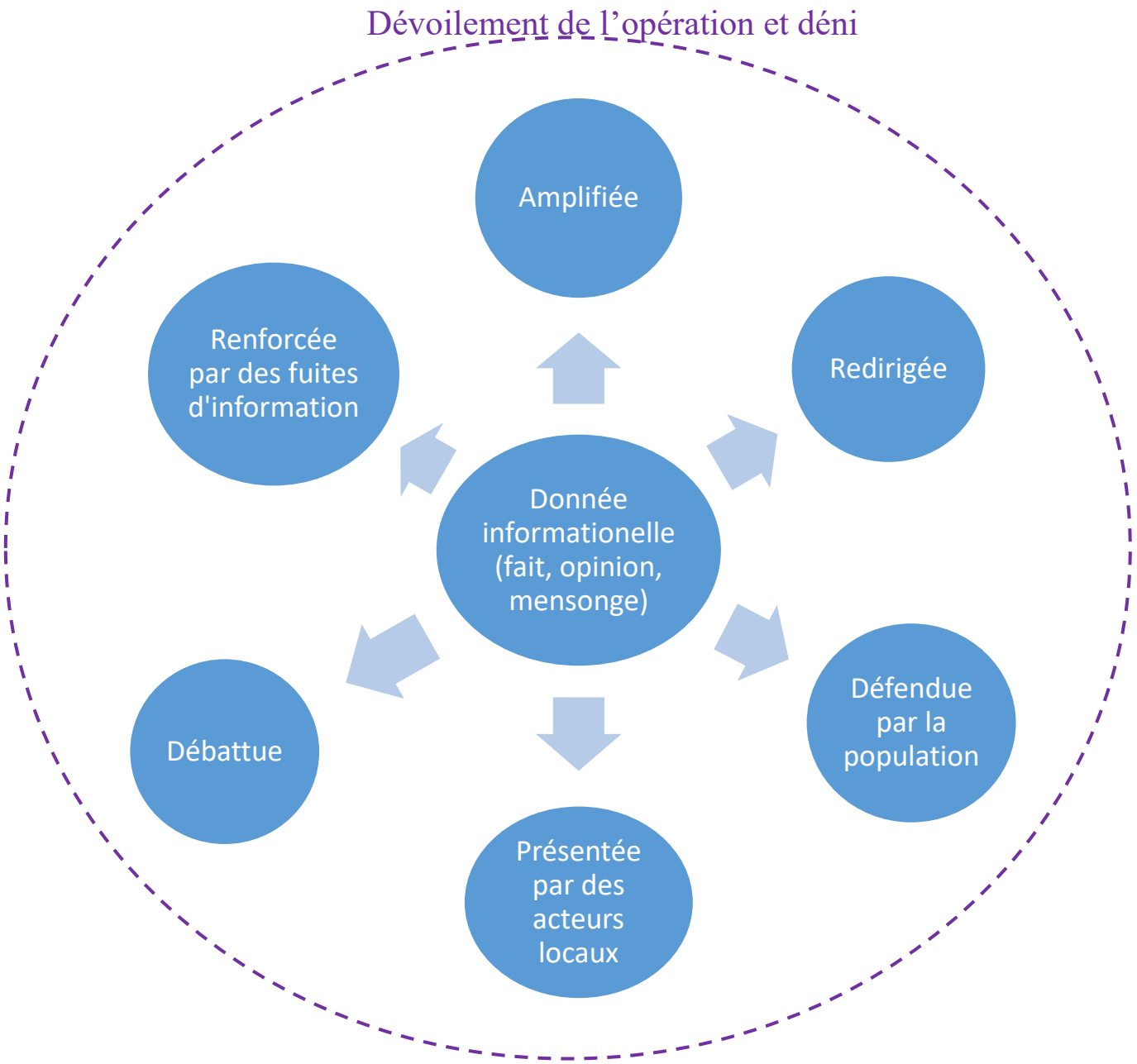
Sur cette donnée fondamentale, une série d'actions est entreprise pour injecter à des doses croissantes cette vision dans la société ciblée. La donnée peut être amplifiée par des *bots* ou des *trolls*. Elle peut être présentée dans une direction différente, c'est-à-dire redirigée. Par exemple, un faux profil présentera la même information, mais sans en révéler l'origine. Elle peut être débattue sur les réseaux sociaux pour inciter la population à s'engager avec cette information. Elle peut être présentée par des acteurs locaux (et donc plus crédibles) comme des ONGs, des partis politiques, des influenceurs d'*Instagram* ou de *Youtube* ou même des médias occidentaux officiels. Elle peut aussi être défendue publiquement par la population dans le cadre de manifestations ou d'événement de la société civile (débats publics, etc.).

Cet environnement informationnel peut être renforcé par des révélations compromettantes provenant de données volées. Alors que les rumeurs et les demi-vérités se propagent dans l'environnement informationnel, le doute s'est installé. Des révélations chocs peuvent alors sembler confirmer la précédente désinformation. De plus, ces fuites d'informations orchestrées mettent dans l'embarras des individus et des organisations. Elles sont souvent relayées par les médias officiels qui en amplifient la portée.

Par ailleurs, la découverte d'une ingérence extérieure peut avoir comme effet de renforcer le climat de suspicion, de doute et de confusion. Une enquête ou un débat sur la manipulation des données informationnelles peut scinder, diviser, perturber et créer de l'incertitude dans une population exposée à des informations qu'elle a de la difficulté à confirmer ou infirmer. En effet, les acteurs impliqués nieront continuellement et se serviront de cet enjeu pour accuser leurs adversaires de paranoïa, de russophobie ou de détourner l'attention des véritables préoccupations du peuple. Cela continue de miner la crédibilité de médias et de politiciens pour une partie de la population.

À partir du moment où des opinions sont acceptées, le sujet devrait théoriquement choisir l'action conforme à ses nouvelles croyances. Il agira ainsi conformément aux volontés du Kremlin. Il est à noter que la paralysie de l'indécision et de l'inaction peut aussi servir les intérêts de la Russie. Autant la mauvaise décision que l'absence de décision sont des éléments de contrôle réflexif.

- Le schéma #5 illustre la structure des stratégies de manipulation de l'information.



h. Séquence chronologique du modèle stratégique

La logique de déploiement des opérations d'information implique une séquence d'actions suivant un ordre chronologique. Cette séquence n'est pas suivie rigidement. Les actions se chevauchent parfois et obéissent à une réalité plus organique. L'étude de cas révèle toutefois que cette structure est représentative du déroulement de ces opérations. Cette séquence a six étapes :

1. Les opérations d'informations débutent par la collecte ou le vol d'informations sensibles. Les chaînes d'information, les activités sur les médias sociaux et autres fausses nouvelles doivent toutes procéder à une collecte d'information pour connaître les sujets d'actualité, les controverses, les sensibilités et les vulnérabilités socio-politiques. Par exemple, afin de manipuler le président géorgien, le renseignement russe devait avoir monté un profil détaillé de son tempérament. Sur la base de ces informations, l'État a pu déployer une opération psychologique à son égard. De façon semblable, pour que la désinformation en Ukraine vise le thème du fascisme, les responsables de l'information russe devaient connaître et collecter des données sur l'organisation *Right Sector* afin de présenter ce mouvement à tendance fasciste comme étant plus influent qu'il ne l'était véritablement. De même, des agents russes se sont présentés sur le sol américain deux ans avant les élections américaines de 2016 pour collecter des informations sur la situation sociale, culturelle et politique. Les opérations aux États-Unis, en France et en Allemagne ont révélé le vol d'informations sensibles dans les phases précédent le déploiement de la propagande/désinformation ou chevauchant cette phase. Comme l'exposait la théorie du contrôle réflexif, l'information doit être basée sur les schèmes de pensée socio-culturels de la cible. Ces schèmes doivent d'abord être un objet d'étude.

2. Sur la base de ces connaissances, une campagne de propagande et de désinformation adaptée à la société ciblée peut être conçue. Cette campagne peut se servir de n'importe quel canal de communication pour diffuser son message. Dans les opérations d'intensité élevée, comme en Ukraine, des informations peuvent être disséminé directement par messages textes dans les cellulaires de citoyens ou de soldats. La propagande et la désinformation doivent être considérées comme des constantes. Elles sont au cœur des opérations d'information et font maintenant partie de l'environnement

informationnel de toutes les sociétés occidentales. Ce phénomène a été recensé dans chaque opération de l'étude de cas. La propagande et la désinformation constituent, avec la collecte d'informations, un cycle d'activité continu pour les agents d'information russes.

3. Ce processus fondamental est le matériel que les nouvelles techniques du cyberespace permettent de manipuler. Les *bots* et les *trolls* utilisent ces données pour en magnifier l'influence. C'est ainsi que le jour du référendum sur le *Brexit* la tâche des *bots* et des *trolls* était essentiellement de retweeté du contenu favorable au *Brexit*. De même, les *trolls* russes arpentent les médias sociaux et les forums d'Ukraine pour commenter les discussions, repartager de l'information et inciter à agir sur cette information, par exemple, en appelant à une troisième révolution contre le gouvernement.

4. Dans cet environnement confus, les agents d'information du Kremlin peuvent tenter de manipuler ou recruter des acteurs locaux. Ceux-ci sont vulnérables par les mêmes quatre facteurs du recrutement par les espions : argent, idéologie, compromission, égo.[331] Ainsi, un parti politique peut partager une idéologie commune à celle de Moscou (comme plusieurs partis européens) ou être influencé à prendre certaines positions par suite de relations financières (ce dont le Front National est soupçonné). La corruption permet de déstabiliser l'Ukraine. De plus, certains acteurs font l'erreur de se compromettre, par exemple lors de rencontres secrètes avec des représentants russes (comme Trump jr.), s'exposant ainsi à des tentatives de recrutement. Ces acteurs renforcent et propagent plus profondément la propagande, la désinformation ou endommagent la confiance sociale.

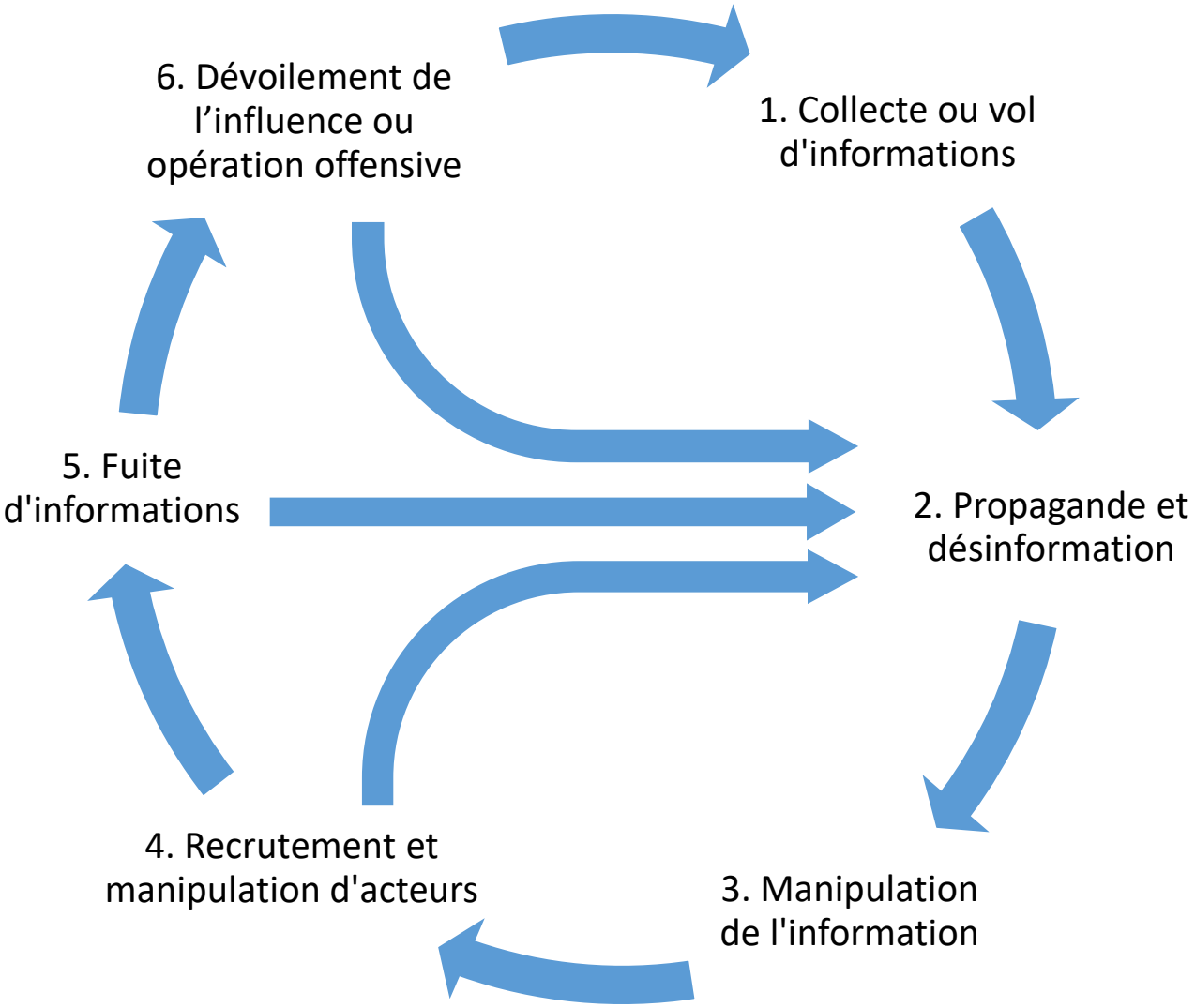
5. Le vol d'informations peut mener à des révélations embarrassantes pour certains acteurs clés. Les fuites d'informations aux États-Unis et en France ont eu lieu la veille des élections. Ce puissant effet à usage limité est déclenché à des périodes qui en maximiseront l'impact, soit vers la fin d'une opération, au moment où les individus s'apprêtent à prendre la décision clé ciblée par Moscou. Ces fuites permettent à la fois de renforcer la propagande et la désinformation déjà émises et d'être le sujet de nouvelles attaques informationnelles.

---

[331] Suivant l'acronyme MICE, en anglais. R. Burkett (2013), *An Alternative Framework for Agent Recruitment: From MICE to RASCLS*, Studies in Intelligence, 57(1), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-57-no.-1-a/vol.-57-no.-1-a-pdfs/Burkett-MICE%20to%20RASCALS.pdf

6. Vers la fin ou après l'opération, il est peu probable que les actions effectuées restent secrètes. La désinformation permet d'ajouter une nouvelle couche de confusion autour du dévoilement des actions russes. Elles sont l'occasion de diviser à nouveau la société ciblée entre les partisans du gouvernement et ses opposants (comme aux États-Unis). De plus, la découverte que des acteurs ont été compromis diminuera la confiance envers l'État et la société. Dans certaines circonstances, la tentative d'influence peut aussi mener à une opération offensive (comme en Géorgie et en Ukraine).

- Le cycle #6 illustre le processus structurel de succession de ces étapes.



i. Rôle stratégique du cyberespace

> In an extreme view, the world can be seen as only connections, nothing else. We think of a dictionary as the repository of meaning, but it defines words only in terms of other words. I liked the idea that a piece of information is really defined only by what it's related to, and how it's related.[332]
>
> - Tim Berners-Lee

L'utilisation massive du cyberespace par la population a permis l'apparition de nouvelles stratégies pour les opérations d'information. Ces stratégies ont développé une synergie avec les précédentes méthodes de propagande et de désinformation. Cette intégration a créé une nouvelle dynamique. Deux éléments fondamentaux de cet environnement informationnel rendent cette dynamique efficace :

1. La vulnérabilité des informations personnelles
2. La facilité de dissimuler derrière un faux profil la propagation et la manipulation d'informations trompeuses ou mensongères.

L'ironie étant qu'alors que nos sociétés prétendent avoir de meilleures capacités de surveillance, ce qu'elles surveillent se dérobe plus facilement à leur regard. Le nœud du problème est l'effet du cyberespace dans le rapport des sociétés à la vérité. Ce qui se dérobe justement est cette vérité, se recouvrent de multiples couches de fausses apparences. L'ensemble des modèles présentés permettent de rendre compte d'une seule réalité : les stratégies du cyberespace pour dissimuler la vérité par des apparences avantageuses politiquement. Le cyberespace est maintenant le médium dominant par lequel la réalité objective atteint les sujets pensants.[333] Ce médium est donc le terrain principal de la guerre de l'information. Cette médiation permet de transformer une réalité objective

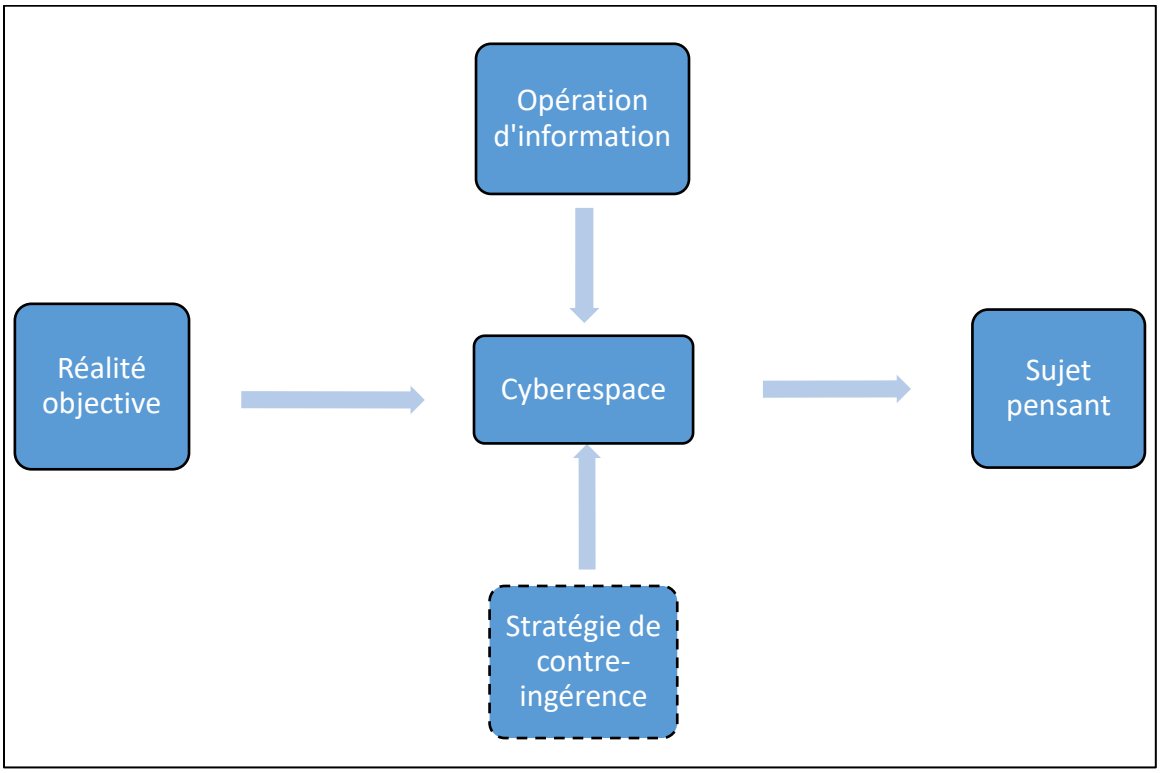
[332] G. Youngs (2007), *Global Political Economy in the Information Age*, London and New York, Routledge, p.44, https://www.taylorfrancis.com/books/9780203964064

[333] J. Mander et K. Young (2017), *Digital vs. Traditional Media Consumption*, Global Web Index, p.8, https://cdn2.hubspot.net/hubfs/304927/Downloads/Digital%20vs%20Traditional%20Summary%20-%20Q1%202017.pdf

désavantageuse en une réalité subjective avantageuse. L'abondance de son accès par une multiplicité d'acteurs rend ce terrain chaotique, confus et riche en opportunités.

Dans sa plus simple expression conceptuelle, le cyberespace est le lieu d'expression et de transformation des perceptions subjectives de la réalité objective. Les opérations d'information sont, au niveau le plus général, une stratégie d'influence de ces perceptions à des fins politiques. La particularité des opérations d'information russes est de faire usage d'une stratégie multidimensionnelle alliant la confusion et la méfiance pour paralyser l'action avec la propagande et la désinformation pour réorienter les décisions. Il reste à voir si les pays occidentaux seront capables de développer des stratégies de contre-ingérence efficaces?

- Le modèle #7 illustre conceptuellement le rôle du cyberespace dans la médiation informationnelle.



VIII. Conclusion – que réserve le futur ?

> Power is in tearing human minds to pieces and putting them together again in new shapes of your own choosing.[334]
>
> - George Orwell

a. Une politique de sécurité informationnelle canadienne?

Un cadre conceptuel a été proposé pour expliquer le fonctionnement des opérations d'information de la Russie. Il peut servir à trois choses :

1. Rendre compte de leur logique inhérente.
2. Définir leurs actions possibles.
3. Prévoir les activités futures de la Russie dans sa guerre de l'information.

La logique présentée est évidemment soumise à la critique. Elle n'est valide qu'en tant qu'elle définit fidèlement la structure de ces opérations. Le deuxième point est explicatif en ce qu'il permet de comprendre et cerner l'environnement d'action. Tout modèle présentant plus clairement et expliquant mieux ces opérations pourrait le supplanter. La force du modèle développé est toutefois de présenter une analyse processuelle. En effet, une compréhension du cycle de déploiement de ces opérations était manquante. De plus, centrer l'analyse de cette stratégie sur la donnée informationnelle est beaucoup plus conforme au mode de pensée des théoriciens russes. Ainsi, un modèle montrant le processus de manipulation de l'information, de même que le cycle de mise en œuvre de cette manipulation permet d'expliquer comment le Kremlin emploi les opérations d'information.

Le véritable test du bien-fondé de l'analyse et du modèle est cependant de déterminer s'il aide à prédire les opérations futures de la Russie et à formuler des contre-stratégies d'ingérence. Une compréhension juste de la situation est inutile si elle ne mène pas à des gestes bénéfiques. En ce sens, c'est notre espoir que le Canada se dote éventuellement d'une politique de cyber sécurité centrée sur la sécurité informationnelle,

[334] Orwell (1948), *1984*, Planet eBook, p.336, https://www.planetebook.com/free-ebooks/1984.pdf

plutôt que sur celle des réseaux[335]. Alors que l'approche occidentale dominante se concentre sur la protection de l'infrastructure (les réseaux) permettant le passage de l'information, une approche axée sur le contenu (l'information) aurait une conception plus vaste de la sécurité en incluant notamment la promotion des médias de qualité, la régulation des conversations virtuelles et un meilleur contrôle des accès aux réseaux publics (pour les *trolls*, les *bots* et les agents étrangers).

b. Évolution des opérations d'information russes

Ces opérations ont un plus grand impact lorsque la cible ignore qu'elle est visée. En ce sens, la diffusion de connaissances à tous les niveaux de la société et de l'État concernant l'ingérence russe sert à se prémunir contre celle-ci. Il était ainsi prévisible que ces opérations diminuent en intensité, en attendant que l'attention publique soit distraite par un nouvel objet de curiosité. Il est probable que ces opérations dans leur forme actuelle ne réapparaissent plus significativement sur notre radar pour un certain temps. Lorsqu'elles se réactiveront, elles auront à la fois appris des leçons de l'expérience passée et intégré les nouveaux outils offerts par l'évolution constante des technologies de l'information.

Parmi ces outils, l'intelligence artificielle est le plus préoccupant. L'utilisation de *deep fakes*, en particulier, tromperait avec plus d'efficacité le jugement commun.[336] La capacité d'automatiser des processus est en croissance. Ce n'est qu'une question de temps avant que la désinformation s'autonomise à une plus grande échelle tout en augmentant en qualité. En l'absence de dissuasion efficace, les contraintes aux opérations d'information sont essentiellement au niveau des ressources. La création de contenu trompeur de qualité doit encore se faire par des mains humaines.[337] La progression des capacités techniques pourrait signifier une augmentation massive de la quantité d'informations trompeuses diffusées et manipulées.

---

[335] Ministère de la Sécurité publique (2018), *National Cyber Security Strategy Canada's Vision for Security and Prosperity in the Digital Age*, Gouvernement du Canada, p.4, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf

[336] M. J. Blitz (2018), *Lies, Line Drawing, and (Deep) Fake News*, Oklahoma Law Review, 71(1), p.62.

[337] D. Wise (2017), *Only Human Hand Can Craft Effective Information Offensives*, Cipher Brief.

Le signal du retour en force ou non des opérations d'information russes sera détectable sur le chemin menant aux élections présidentielles américaines du 3 novembre 2020. Il sera possible d'évaluer si de nouvelles techniques ont été intégrées, si la stratégie a été modifiée et si l'occident a tiré des leçons de ses vulnérabilités.

c. Avenues de recherches futures

Les outils d'analyse qui ont été développés pourront servir à mieux comprendre les opérations d'information qui ont lieu en ce moment même. À l'approche des élections fédérales au Canada en octobre 2019, le gouvernement a émis plusieurs mises en garde contre l'ingérence de la Russie. Le Centre de la sécurité des télécommunications et le Service canadien du renseignement de sécurité ont déployés des ressources pour prévenir cette ingérence. De plus, un groupe de hauts fonctionnaires a été réuni pour surveiller l'interférence extérieure lors des élections et, si nécessaire, alerter le gouvernement et la population sur celle-ci.[338] Le modèle descriptif s'étant dégagé de cette recherche pourra être appliqué pour déterminer le niveau d'interférence, la structure de cette interférence ainsi que les actions russes qui devraient logiquement suivre ce qui est observé à un instant donné. Son application à des études de cas supplémentaires permettra aussi de l'améliorer afin de le rendre plus exact et performant. De plus, la compréhension se dégageant de ce mémoire pourrait être amené plus en profondeur sur le terrain des débats théoriques sur les conceptions du pouvoir en relations internationales. En effet, la section théorique exposait entre autres une remise en question par certains auteurs de la pertinence des modèles théoriques du XXe siècle pour permettre de comprendre et d'expliquer les luttes de puissance dans le cyber environnement. Une exploration de ce territoire en fonction des données retirées de la présente recherche pourrait contribuer à ce débat.

Ce modèle est, par ailleurs, dans une forme embryonnaire. Il détaille les grandes lignes de la structure de ces opérations, mais laisse de nombreux détails dans une zone

[338] M. Vastel (2019), *Un système de défense contre l'ingérence lors des élections*, Le Devoir, 31 janvier, https://www.ledevoir.com/politique/canada/546715/elections-le-systeme-canadien-de-defense-contre-l-ingerence-russe

d'ombre. Chaque composante du cycle processuel[339] serait intéressante à détailler avec son cycle et sa structure propre. Quel est le processus de collecte d'information? Quel est le processus de manipulation des acteurs qu'utilisent les agents d'information russes? Ainsi, le modèle gagnerait à être approfondi, détaillé et complexifié. Il ne faut pas oublier qu'une modélisation semblable existe certainement dans les documents classifiés d'ordres stratégique, opérationnel et tactique des agences de sécurité et de défense russes. C'était l'ambition de cette recherche d'en clarifier la teneur. Il reste maintenant à améliorer par des études de cas subséquentes ce qui a été bâti dans ce mémoire, de même qu'à aider une réponse gouvernementale appropriée.

[339] 1. Collecte ou vol d'informations; 2. Propagande et désinformation; 3. Manipulation de l'information; 4. Recrutement et manipulation d'acteurs; 5. Fuite d'informations; 6. Dévoilement de l'influence ou opération offensive

IX. Annexes

ANNEXE 1

PHYSICAL AND VIRTUAL DIMENSIONS OF CYBERPOWER

TARGETS OF CYBERPOWER		
	INTRA-CYBERSPACE	EXTRA-CYBERSPACE
INFORMATION INSTRUMENTS	Hard : denial of service attacks Soft: setting of norms and standards	Hard: attack on SCADA systems Soft: public diplomacy campaign to sway opinion
PHYSICAL INSTRUMENTS	Hard : government control of companies Soft : software to help human rights activists	Hard: bomb routers or cutting of cables Soft: protests to name and shame cyberproviders

Source: J. S. Nye, *The Future of Power*, New York, Public Affairs, p.127.

ANNEXE 2

THREE FACES OF POWER IN THE CYBERDOMAIN

FIRST FACE A INDUCING B TO DO WHAT B WOULD INITIALLY OTHERWISE NOT DO
Hard: denial of service attacks, insertion of malware, SCADA disruption, arrest of bloggers Soft: information campaign to change initial preferences of hackers, recruitment of members of terrorist organizations
SECOND FACE A PRECLUDING B'S CHOICE BY EXCLUDING B'S STRATEGIES
Hard: firewalls, filters, and pressure on companies to exclude some ideas Soft: self-monitoring of ISPs and search engines, ICANN rules on domain names, widely accepted software standards
THIRD FACE A SHAPING B'S PREFERENCES SO THAT SOME STRATEGIES ARE NEVER EVEN CONSIDERED
Hard: threats to punish bloggers who disseminate censored material Soft: information to create preferences (such as stimulation of nationalism and patriotic hackers), development of norms of revulsion (such as child pornography)

Source: J. S. Nye, *The Future of Power*, New York, Public Affairs, p.130.

X. Bibliographie

AJIR et VAILLIANT (2018), *Russian Information Warfare : Implications for Deterrence Policy*, Strategic Studies Quarterly, 12(3), https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Ajir.pdf

ALLEN et MOORE (2018), *Victory without Casualties: Russia's Information Operations*, Parameters, 48(1), https://ssi.armywarcollege.edu/pubs/parameters/issues/Spring_2018/9_Allen_VictoryWithoutCasualties.pdf

APPLEBAUM, POMERANTSEV , SMITH et COLLIVER (2017), *"MAKE GERMANY GREAT AGAIN" Kremlin, Alt-Right and International Influences in the 2017 German Elections*, Institute for Global Affairs, London School of Economics, http://www.lse.ac.uk/iga/assets/documents/arena/2017/Make-Germany-Great-Again-ENG-061217.pdf

AVGUSTIN et NURNUS (dir.), *Realism in Practice*, E-International Relations Publishing, https://eprints.ncl.ac.uk/file_store/production/245064/D474E3F6-4CEE-45C9-AC88-BF59E19C0ADC.pdf

BAKER, FERMAINT et NEFF (2013), *The Russia-Georgia War of 2008: Information Operations Case Study Analysis*, https://www.academia.edu/11903525/The_Russia-Georgia_War_of_2008_Information_Operations_Case_Study_Analysis

BALTIC MONITOR (2018), *Russia reacts to Trident Juncture 18*, Warsaw Institute, https://warsawinstitute.org/russia-reacts-trident-juncture-18/

BEST (2013), *The Ethnic Russian Minority: A Problematic Issue in the Baltic States*, Verges: Germanic and Slavic Studies in review, 2(1), https://journals.uvic.ca/index.php/verges/article/view/11634

BEUTH, BIERMANN, KLINGST et STARK (2017), *Cyberattack on the Bundestag: Merkel and the Fancy Bear*, Zeit Online, https://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia/komplettansicht

BEUTH, BROST, DAUSEND et al. (2017), *War Without Blood*, Zeit Online, https://www.zeit.de/digital/internet/2017-02/bundestag-elections-fake-news-manipulation-Russia-hacker-cyberwar/komplettansicht

BLANK (2008), *Web War I: Is Europe's First Information War a New Kind of War?,* Comparative Strategy, 27(3), https://www.tandfonline.com/doi/pdf/10.1080/01495930802185312?needAccess=true

BLITZ (2018), *Lies, Line Drawing, and (Deep) Fake News*, Oklahoma Law Review, 71(1), https://digitalcommons.law.ou.edu/cgi/viewcontent.cgi?article=1343&context=olr

BRATTBERG et MAURER (2018), *RUSSIAN ELECTION INTERFERENCEL Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf

BRAW (2018), *How to Deal With Russian Information Warfare? Ask Sweden's Subhunters,* Defense One, https://www.defenseone.com/ideas/2018/04/how-deal-russian-information-warfare-ask-sweden/147154/

BREMNER (2016), *Le Pen's party asks Russia for €27m loan*, The Sunday Times, https://www.thetimes.co.uk/article/le-pens-party-asks-russia-for-euro27m-loan-kzxq8m7s30v

BROWN et ECKERSLEY, *The Oxford Handbook of International Political Theory*, Oxford University Press.

BURKETT (2013), *An Alternative Framework for Agent Recruitment: From MICE to RASCLS*, Studies in Intelligence, 57(1), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-57-no.-1-a/vol.-57-no.-1-a-pdfs/Burkett-MICE%20to%20RASCALS.pdf

CAVELTY, MAUER et KRISHNA-HENSEL (dir.), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*, Ashgate Publishing.

CHIVVIS (2017), *Understanding Russian "Hybrid Warfare" and What Can be Done About It*, RAND Corporation, Testimony presented before the House Armed Services Committee,

https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

CHOUCRI et GOLDSMITH (2012), *Lost in cyberspace: Harnessing the Internet, international relations, and global security*, Bulletin of the Atomic Scientists, 68(2), https://journals.sagepub.com/doi/pdf/10.1177/0096340212438696

CLOGG (1997), *Disinformation in Chechnya: an anatomy of a deception*, Central Asian Survey, 16(3).

CNN (2019), *2016 Presidential Campaign Hacking Fast Facts*, CNN Library, https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html

COLE (2018), THE HARD EDGE OF SHARP POWER: *Understanding China's Influence Operations Abroad*, Macdonald-Laurier Institute, https://macdonaldlaurier.ca/files/pdf/20181022_MLI_China's_Influence_(Cole)_PAPER_WebreadyF.pdf

COLLIER (2016), *Latvia in the Crosshairs: Russian Information Warfare and Appropriate Countermeasures*, Small Wars Journal, https://smallwarsjournal.com/jrnl/art/latvia-in-the-crosshairs-russian-information-warfare-and-appropriate-countermeasures#_edn9

COMEY (2017), *Full Transcript and Video: James Comey's Testimony on Capitol Hill*, The New York Times, https://www.nytimes.com/2017/06/08/us/politics/senate-hearing-transcript.html

DAHL (2012), *Partner number one or NATO ally twenty-nine? Sweden and NATO post-Lybia*, Research Division – Nato Defense College, No.82, https://www.files.ethz.ch/isn/153549/rp_82.pdf

DARCZEWSKA (2014), *The anatomy of Russian information warfare*, Centre for Eastern Studies (OSW), http://aei.pitt.edu/57173/1/42.pdf

DAVIS (2018), *RUSSIAN MEDDLING IN ELECTIONS AND REFERENDA IN THE ALLIANCE*, NATO Parliamentary Assembly, Science and Technology Committee (STC), https://www.nato-pa.int/document/2018-russian-meddling-elections-and-referenda-alliance-davis-report-181-stc-18-e-fin

DAWSON et INNES (2019), *How Russia's Internet Research Agency Built its Disinformation Campaign*, The Political Quarterly, 90(2), https://onlinelibrary.wiley.com/doi/full/10.1111/1467-923X.12690

DEFENSE NEWS (2016), *Sweden Adopts Tougher Military Strategy Doctrine*, https://www.defensenews.com/global/europe/2016/03/17/sweden-adopts-tougher-military-strategy-doctrine/

DEIBERT, ROHOZINSKI et CRETE-NISHIHATA (2012), *Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war*, Security Dialogue, 43(1), https://journals.sagepub.com/doi/pdf/10.1177/0967010611431079

DIRESTA, ALBRIGHT, JOHNSON et al. (2018), *The Tactics & Tropes of the Internet Research Agency*, New Knowledge, https://cdn2.hubspot.net/hubfs/4326998/ira-report-rebrand_FinalJ14.pdf

DUXBURY (2016), *Sweden Ratifies NATO Cooperation Agreement*, The Wall Street Journal, https://www.wsj.com/articles/sweden-ratifies-nato-cooperation-agreement-1464195502

ERIKSSON et GIACOMELLO (2006), *The Information Revolution, Security, and International Relations: (IR)relevant Theory?,* International Political Science Review, 27(3), https://journals.sagepub.com/doi/pdf/10.1177/0192512106064462

EU vs DISINFORMATION (2019), *Disinformation Review*, European External Action Service East Stratcom Task Force, https://euvsdisinfo.eu/

FERNQUIST, KAATI, SCHROEDER et al. (2018), *Bots and the Swedish election: A study of automated accounts on Twitter*, Swedish Defence Research Agency (FOI), https://www.foi.se/rapportsammanfattning?reportNo=FOI%20MEMO%206466

FERRAND (2017), *Ne laissons pas la Russie déstabiliser la présidentielle en France !,* Le Monde, https://www.lemonde.fr/election-presidentielle-2017/article/2017/02/14/ne-laissons-pas-la-russie-destabiliser-la-presidentielle-en-france_5079213_4854003.html

FOURNAS (2017), *Présidentielle: 14 fake news qui circulent sur Emmanuel Macron*, 20 minutes France, https://www.20minutes.fr/high-tech/2058855-20170428-presidentielle-14-fake-news-circulent-emmanuel-macron

FRANKE (2015), *War by non-military means Understanding Russian information warfare*, Swedish Defence Research Agency (FOI), http://johnhelmer.net/wp-content/uploads/2015/09/Sweden-FOI-Mar-2015-War-by-non-military-means.pdf

GALEOTTI (2016), *Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?,* Small Wars & Insurgencies, 27(2).

GAUTHIER et BOURGEOIS (dir.) *Recherche sociale: De la problématique à la collecte de données*, 6e édition, Québec, Presses de l'Université du Québec.

GEERS (dir.), *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallinn, NATO CCD COE Publications, https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf

GILES (2016), *Handbook of Russian Information Warfare*, NATO Defense College, http://www.ndc.nato.int/news/news.php?icode=995

GILES, SHERR et SEABOYER (2018), *Russian Reflexive Control*, Royal Military College of Canada, Rapport pour Defence Research and Development Canada, http://cradpdf.drdc-rddc.gc.ca/PDFS/unc323/p807769_A1b.pdf

GOLLEY, JAIVIN, FARRELLY et STRANGE (dir.), *Power*, ANU Press, https://www.jstor.org/stable/j.ctvfrxqkv.21

GORODNICHENKO, PHAM et TALAVERA (2018), *Social media, sentiment and public opinions: Evidence from #Brexit and #USElection*, National Bureau of Economic Research, Working Paper No. 24631, https://rahwebdav.swan.ac.uk/repec/pdf/wp2018-01.pdf

HALL (2017), *General Chaos is the Kremlin's Favorite Candidate*, Cipher Brief, https://www.thecipherbrief.com/general-chaos-kremlins-favorite-candidate?fbclid=IwAR29mpcZWUqj5X4mwNEMEayduuqyQvjLuQPHTELzKuJt0QfBWkkHLqdS8mw

HARDING (2007), *Russia up in arms after Estonians remove statue of Soviet soldier*, The Guardian, https://www.theguardian.com/world/2007/apr/28/russia.lukeharding

HEDMAN, SIVNERT, KOLLANYI et al. (2018), *News and Political Information Consumption in Sweden: Mapping the 2018 Swedish General Election on Twitter*, DATA MEMO 2018.3, Project on Computational Propaganda, University of Oxford,

https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/09/Hedman-et-al-2018.pdf

HEICKERÖ (2010), *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, Swedish Defence Research Agency (FOI), http://www.highseclabs.com/data/foir2970.pdf

HEINRICH et TANAEV (2009), *Georgia & Russia : Contradictory Media Coverage of the August War*, Caucasian Review of International Affairs, 3(3), http://www.cria-online.org/Journal/8/Done_Georgia-Russia_Contradictory%20Media%20Coverage%20of%20the%20August%20War_Heinrich_Tanaev.pdf

HELMUS, BODINE-BARON, RADIN, MAGNUSON et al. (2018), *Russian Social Media Influence Understanding Russian Propaganda in Eastern Europe*, RAND Corporation, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf

HERD (2000), *The 'counter-terrorist operation' in Chechnya: 'Information warfare' aspects*, The Journal of Slavic Military Studies, 13(4).

HERN, DUNCAN et BENGTSSON, *Russian 'troll army' tweets cited more than 80 times in UK media*, The Guardian, https://www.theguardian.com/media/2017/nov/20/russian-troll-army-tweets-cited-more-than-80-times-in-uk-media

HERZOG (2011), Revisiting *the Estonian Cyber Attacks: Digital Threats and Multinational Responses,* Journal of Strategic Security, 4(2), p.51, https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss

HOLLIS (2011), *Cyberwar Case Study: Georgia 2008*, Small Wars Journal, https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

HOWARD, BRADSHAW, KOLLANYI et al. (2017), *Junk News and Bots during the French Presidential Election: What Are French Voters Sharing Over Twitter?,* DATA MEMO 2017.3, Project on Computational Propaganda, University of Oxford, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/04/What-Are-French-Voters-Sharing-Over-Twitter-v9.pdf

HOWARD, GANESH et LIOTSIOU (2018), *The IRA, Social Media and Political Polarization in the United States, 2012-2018*, Working Paper 2018.2 Project on Computational Propaganda, University of Oxford, https://comprop.oii.ox.ac.uk/research/ira-political-polarization/

IASIELLO (2017), *Russia's Improved Information Operations: From Georgia to Crimea*, Parameters, 47(2), https://publications.armywarcollege.edu/pubs/3368.pdf

ISNARTI (2016), *A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War*, Andalas Journal of International Studies, 5(2), http://ajis.fisip.unand.ac.id/index.php/ajis/article/view/53/43

JOHNSON (2007), *Toward a Functional Model of Information Warfare*, CIA Library, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/warfare.html

KELLO (2013), *The Meaning of the Cyber Revolution: Perils to Theory and Statecraft*, International Security, 38(2), https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00138

KIVIRÄHK (2014), *Integrating Estonia's Russian-Speaking Population: Findings of National Defense Opinion Surveys*, International Centre for Defence and Security: Estonia, https://icds.ee/wp-content/uploads/2014/Juhan_Kivirahk_-_Integrating_Estonias_Russian-Speaking_Population.pdf

KRAGH et ÅSBERG (2017), *Russia's strategy for influence through public diplomacy and active measures: the Swedish case*, Journal of Strategic Studies, 40(6), https://www.tandfonline.com/doi/full/10.1080/01402390.2016.1273830

KROL (2017), *Russian Information Warfare in the Baltic States — Resources and Aims*, Warsaw Institute, paragraphe: Narratives most widespread in the media, https://warsawinstitute.org/russian-information-warfare-baltic-states-resources-aims/

KUCERA (2011), *Condoleezza Rice Warned Georgian Leader on War With Russia*, The Atlantic, https://www.theatlantic.com/international/archive/2011/11/condoleezza-rice-warned-georgian-leader-on-war-with-russia/248560/

LAURINAVIČIUS (2018), *A Guide to the Russian Tool Box of Election Meddling*, International Election Study Center (IESC), http://iesc.lt/app/uploads/2018/10/IESC_Guide_ToolBox_2018_FINAL.pdf

LE MONDE (2015), *Financement du FN : des hackers russes dévoilent des échanges au Kremlin*, https://www.lemonde.fr/les-decodeurs/article/2015/04/02/fn-des-hackers-russes-devoilent-des-echanges-au-kremlin_4608660_4355770.html

LIU (2018), *What Sharp Power? It's nothing but ''unsmart'' power*, USC Center of Public Diplomacy, https://www.uscpublicdiplomacy.org/blog/what-sharp-power-it%E2%80%99s-nothing-%E2%80%9Cunsmart%E2%80%9D-power

LLEWELLYN, CRAM, FAVERO et HILL, *For Whom the Bell Trolls: Troll Behaviour in the Twitter Brexit Debate*, JCMS: Journal of Common Market Studies, https://arxiv.org/pdf/1801.08754.pdf.

MANDER et YOUNG (2017), *Digital vs. Traditional Media Consumption, Global Web Index*, https://cdn2.hubspot.net/hubfs/304927/Downloads/Digital%20vs%20Traditional%20Summary%20-%20Q1%202017.pdf

MANDRAUD (2017), *À Moscou, Vladimir Poutine adoube Marine Le Pen*, Le Monde, https://www.lemonde.fr/election-presidentielle-2017/article/2017/03/24/marine-le-pen-recue-par-vladimir-poutine-a-moscou_5100247_4854003.html

MANJIKIAN (2010), *From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik*, International Studies Quarterly, 54, https://academic.oup.com/isq/article/54/2/381/1795973

MARTIN (1982), *Disinformation: An instrumentality in the propaganda arsenal*, Political Communication, 2(1), https://www.tandfonline.com/doi/abs/10.1080/10584609.1982.9962747

MAYBAUM, OSULA et LINDSTRÖM, *7th International Conference on Cyber Conflict: Architectures in Cyberspace,* Tallinn, NATO CCD COE Publications, https://ccdcoe.org/uploads/2018/10/CyCon_2015_book.pdf

MCGUINNESS (2016), *Russia steps into Berlin 'rape' storm claiming German cover-up*, BBC News, https://www.bbc.com/news/blogs-eu-35413134

MEISTER (2016), *The "Lisa case": Germany as a target of Russian disinformation*, NATO Review magazine, https://www.nato.int/docu/review/2016/also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm

MERRIAM-WEBSTER DICTIONARY, *Propaganda*, https://www.merriam-webster.com/dictionary/propaganda

MINISTÈRE DE LA DÉFENSE NATIONALE (2009), *CFJP 01 Canadian Military Doctrine*, Gouvernement du Canada, http://publications.gc.ca/collections/collection_2010/forces/D2-252-2009-eng.pdf

MINISTÈRE DE LA SÉCURITÉ PUBLIQUE (2018), *National Cyber Security Strategy Canada's Vision for Security and Prosperity in the Digital Age*, Gouvernement du Canada, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf

MÖLDER et SAZONOV (2018), *Information Warfare as the Hobbesian Concept of Modern Times — The Principles, Techniques, and Tools of Russian Information Operations in the Donbass*, The Journal of Slavic Military Studies, 31(3) https://www.tandfonline.com/doi/full/10.1080/13518046.2018.1487204

MUELLER III (2018), *UNITED STATES OF AMERICA v. INTERNET RESEARCH AGENCY LLC [and other Defendants]*, United States Department of Justice, https://www.justice.gov/file/1035477/download?fbclid=IwAR3YArxy3bTNVUWrWaI9kZpo34dF_9isYZfG5veSz2MB_OfGz9vZEkkAr3s

MUELLER III (2019), *Report on the investigation into Russian interference in the 2016 Presidential election Volume I of II*, United States Department of Justice, https://www.justsecurity.org/wp-content/uploads/2019/04/Muellller-Report-Redacted-Vol-I-Released-04.18.2019-Word-Searchable.-Reduced-Size.pdf

NIMMO (2016), *Putin's media are pushing Britain for the Brexit*, The Interpreter, http://www.interpretermag.com/putins-media-are-pushing-britain-for-the-brexit/

NIMMO (2017), *#ElectionWatch: Russian Botnet Boosts German Far-Right Posts*, Digital Forensic Research Lab – Atlantic Council, https://medium.com/dfrlab/german-election-russian-botnet-boosts-far-right-posts-45f170bc2321

NIMMO (2017), *The Kremlin's Amplifiers in Germany The activists, bots, and trolls that boost Russian propaganda*, Digital Forensic Research Lab – Atlantic Council, https://medium.com/dfrlab/the-kremlins-amplifiers-in-germany-da62a836aa83

NYE (2002), *The Information Revolution and American Soft Power*, Asia-Pacific Review, 9(1), https://www.tandfonline.com/doi/pdf/10.1080/13439000220141596?needAccess=true

NYE (2004), *Soft Power*, New York, Public Affairs.

NYE (2009), *Get Smart: Combining Hard and Soft Power*, Foreign Affairs, 88(4), https://www.foreignaffairs.com/articles/2009-07-01/get-smart

NYE (2011), *The Future of Power*, New York, Public Affairs.

NYE (2018), *How Sharp Power Threatens Soft Power*, Foreign Affairs, https://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (2017), *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution,* United States Government, https://www.dni.gov/files/documents/ICA_2017_01.pdf

ORENSTEIN (2015), *Putin's Western Allies: Why Europe's Far Right Is on the Kremlin's Side*, Foreign Affairs, https://www.foreignaffairs.com/articles/russia-fsu/2014-03-25/putins-western-allies

ORWELL (1948), *1984*, Planet eBook, https://www.planetebook.com/free-ebooks/1984.pdf

PARMAR et COX (dir.), *Soft Power and US Foreign Policy: Theoretical, historical and contemporary perspectives*, New York, Routledge.

PAUL et MATTHEWS (2016), *The Russian ''Firehose of Falsehood'' Propaganda Model*, Rand Corporation, https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf

PAYNE et MARTIN (2017), *The 21 biggest donors to the Brexit campaign*, Business Insiders, https://www.businessinsider.com/twenty-one-biggest-donors-to-the-leave-brexit-campaign-2017-5

PETERSON (dir.) *Russian Strategic Intentions*, NSI, Inc., rapport pour le Département de la défense des États-Unis, https://nsiteam.com/sma-white-paper-russian-strategic-intentions/

POLYAKOVA et BOYER (2018), *The future of political warfare: Russia, the West, and the coming age of global digital competititon*, BROOKINGS – ROBERT BOSCH FOUNDATION TRANSATLANTIC INITIATIVE, https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf

POLYAKOVA, LARUELLE, MEISTER et BARNETT (2016), *THE KREMLIN'S TROJAN HORSES: Russian Influence in France, Germany, and the United Kingdom*, DINU Patriciu Eurasia Center – Atlantic Council, https://www.atlanticcouncil.org/images/publications/The_Kremlins_Trojan_Horses_web_0228_third_edition.pdf

PRÉEL et MAROT (2017), *Macron accuse Moscou d'ingérence au profit de Fillon et de Le Pen*, Le Devoir, https://www.ledevoir.com/monde/europe/491705/presidentielle-francaise-macron-accuse-moscou-d-ingerence-au-profit-de-fillon-et-de-le-pen

RADWARE (2016), *Attack on Sweden's Media*, Radware, https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/sweden-attack-threat-alert/

RANDIN (2017), *Hybrid Warfare in the Baltics*, RAND Corporation, https://www.rand.org/pubs/research_reports/RR1577.html#download

ROHOZINSKI et DEIBERT (2010), *Liberation vs. Control: The Future of Cyberspace*, Journal of Democracy, 21(4), https://www.journalofdemocracy.org/articles/liberation-vs-control-the-future-of-cyberspace/

ROSS, MOSK, KREIDER et al. (2017), *Russian internet trolls sought to co-opt unwitting American activist*s, ABC News, https://abcnews.go.com/Politics/russian-internet-trolls-sought-opt-unwitting-american-activists/story?id=50570832

SHAFFER, CAREY et STARLING (2017), *Democracy Hacked: A Massive, Pro-Le Pen Disinformation Campaign Hits Twitter, 4chan, and the Mainstream Media*, Data for Democracy, https://medium.com/data-for-democracy/democracy-hacked-a46c04d9e6d1

SHALAL (2017), *Germany challenges Russia over alleged cyberattacks*, Reuters, https://www.reuters.com/article/us-germany-security-cyber-russia/germany-challenges-russia-over-alleged-cyberattacks-idUSKBN1801CA

SHANE (2018), *How Unwitting Americans Encountered Russian Operatives Online*, The New York Times, https://www.nytimes.com/2018/02/18/us/politics/russian-operatives-facebook-twitter.html

STELZENMÜLLER (2017), *The Impact of Russian Interference on Germany's 2017 Elections: Testimony before the U.S. Senate Select Committee on Intelligence*, Brookings Institution, https://www.intelligence.senate.gov/sites/default/files/documents/sfr-cstelzenmuller-062817b.pdf

STRATFOR (2017), *Russia Campaigns for the French Presidency*, Stratfor Worldview, https://worldview.stratfor.com/article/russia-campaigns-french-presidency

STUKAL, SANOVICH, BONNEAU et TUCKER (2017). *Detecting Bots on Russian Political Twitter. Big Data*, 5(4), pp.310-324, https://www.liebertpub.com/doi/10.1089/big.2017.0038

SUN TZU, *The Art of War*, Oxford University Press, 1971.

THE DIGITAL, CULTURE, MEDIA AND SPORT COMMITTEE (2018), *Disinformation and 'fake news': Interim Report*, U.K. House of Commons, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf

THE DIGITAL, CULTURE, MEDIA AND SPORT COMMITTEE (2019), *Disinformation and 'fake news': Final Report*, U.K. House of Commons, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf

THOMAS (1998), *Dialectical versus empirical thinking: Ten key elements of the Russian understanding of information operations*, The Journal of Slavic Military Studies, 11(1), https://www.tandfonline.com/doi/abs/10.1080/13518049808430328

THOMAS (2009), *The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia*, Slavic Military Studies, 22(1). https://www.tandfonline.com/doi/pdf/10.1080/13518040802695241?needAccess=true

THOMAS (2014), *Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?,* The Journal of Slavic Military Studies, 27(1), https://www.tandfonline.com/doi/pdf/10.1080/13518046.2014.874845?needAccess=true

TRANSPARENCY INTERNATIONAL (2019), *Corruption Perception Index 2018*, https://www.transparency.org/cpi2018

UNITED STATES GOVERNMENT (2018), *National Cyber Strategy of the United States of America*, The White House, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

U.S. DEPARTMENT OF DEFENSE (2014), *Joint Publication 3-13 Information Operations*, United States Government, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

U.S. DEPARTMENT OF DEFENSE (2018), *Joint Publication 3-12 Cyberspace Operations*, United States Government, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150

U.S. SENATE COMMITTEE ON FOREIGN RELATIONS (2018), *PUTIN'S ASYMMETRIC ASSAULT ON DEMOCRACY IN RUSSIA AND EUROPE: IMPLICATIONS FOR U.S. NATIONAL SECURITY*, United States Senate, https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

USTINOVA et PIFER (20129), *Time to play hardball on reforming Ukraine's Security Service*, Atlantic Council, https://www.atlanticcouncil.org/blogs/ukrainealert/time-to-play-hardball-on-reforming-ukraine-s-security-service

VANDERBIEST (2017), *Quelle est l'influence russe sur la campagne présidentielle française?* Reputatio Lab, https://www.les-crises.fr/wp-content/uploads/2018/09/1-reputatio-lab-20-04-2018.pdf

VASTEL (2019), *Un système de défense contre l'ingérence lors des élections*, Le Devoir, 31 janvier.

WALKER et LUDWIG (2017), *Sharp Power: Rising Authoritarian Influence*, National Endowment for Democracies, https://www.ned.org/wp-content/uploads/2017/12/Sharp-Power-Rising-Authoritarian-Influence-Full-Report.pdf

WALKOWIAK et HOLMES (2017), *Russia's meddling in the French elections: How and why?,* Election Watch, University of Melbourne, https://electionwatch.unimelb.edu.au/articles/russias-meddling-in-the-french-elections-how-and-why

WALTERS (2015), *Secrecy, publicity and the milieu of security*, Dialogues in Human Geography, 5(3), https://journals.sagepub.com/doi/10.1177/2043820615607766

WEBB (2017), *Brazen Murder in Kiev Chills Russia's Dissidents in Ukraine*, Foreign Policy, https://foreignpolicy.com/2017/03/28/brazen-murder-in-kiev-chills-russias-dissidents-in-ukraine/

WHITE (2018), *Understanding Cyberwarfare Lessons from the Russia-Georgia War*, Modern War Institute at West Point, https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf

WIESLANDER (2018), *Will Sweden's Elections Lead to NATO Membership?,* Atlantic Council, https://www.atlanticcouncil.org/blogs/new-atlanticist/will-sweden-s-elections-lead-to-nato-membership

WILSON III (2008), *Hard Power, Soft Power, Smart Power*, The American Academy of Political and Social Science, 616(1), https://journals.sagepub.com/doi/pdf/10.1177/0002716207312618

WISE (2017), *Only Human Hand Can Craft Effective Information Offensives*, Cipher Brief, https://www.thecipherbrief.com/human-hands-can-craft-effective-information-offensives?fbclid=IwAR3P9FGYfSEOkKK3ZK1_anrzCvJlGf9NDtbPdlfi-Xb1bsX4ezKojGM7OVE

WITTGENSTEIN (1921), *Tractatus logico-philosophicus*, proposition 4.002, Routledge, 2e édition, 2001.

YOUNGS (2007), *Global Political Economy in the Information Age*, London and New York, Routledge, https://www.taylorfrancis.com/books/9780203964064

ZHDANOVA et ORLOVA (2017), *Computational Propaganda in Ukraine: Caught between external threats and internal challenges*, Working Paper 2017.9, Project on Computational Propaganda, University of Oxford, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Ukraine.pdf