Faculté des sciences économiques, sociales, politiques et de communication
École des sciences politiques et sociales (PSAD)

L'influence des cyberattaques russes sur la scène politique dans l'ouest de l'UE : Le cas de l'Espagne et de la France

Auteur : Marta María ZAPICO ALONSO
Promoteur : Benoît RIHOUX
Année académique : 2021 – 2022
Master en Sciences Politiques, orientation générale

« *Je déclare sur l'honneur que ce TFE a été écrit de ma plume, sans avoir sollicité d'aide extérieure illicite, qu'il n'est pas la reprise d'un travail présenté dans une autre institution pour évaluation, et qu'il n'a jamais été publié, en tout ou en partie. Toutes les informations (idées, phrases, graphes, cartes, tableaux, ...) empruntées ou faisant référence à des sources primaires ou secondaires sont référencées adéquatement selon la méthode universitaire en vigueur.*

*Je déclare avoir pris connaissance et adhérer au Code de déontologie pour les étudiants en matière d'emprunts, de citations et d'exploitation de sources diverses et savoir que le plagiat constitue une faute grave***. »**

Marta María Zapico Alonso

Je tenais à adresser mes remerciements à toutes les personnes qui m'ont, de près ou de loin, aider à réaliser au mieux ce travail de fin d'étude.

Je souhaite particulièrement remercier Margaux Repellin pour son aide précieuse et son encadrement tout au long de ce travail.

Je remercie également mon promoteur Benoît Rihoux pour les connaissances qu'il m'a transmises et ses recommandations.

J'adresse mes remerciements aussi à Nicolas Bocquet pour m'avoir donné un avis critique sur mon mémoire.

Finalement, je remercie ma famille et mes amis de m'avoir soutenu et aidé pendant tout le processus, en particulier Elinda, Pierre, Emma et Eva.

ABSTRACT

The rapid development of the fifth domain in recent decades has revealed its essential role in geopolitics. In this context, Russia emerges as one of the main powers in cyberspace given its comparatively advanced capabilities at the international level. This paper will develop Russia's influence through cyberspace outside of its frontiers in two cases. The first one is during the highest peak of the Catalan crisis in Spain in 2017 and second one is the French elections in 2017. We will discover how disruptive cyberattacks can be even if they don't achieve its goal and the necessity to take measures to prevent them.

KEY WORDS

Russia, Cyberattack, disinformation, Catalonia, France.

RÉSUMÉ

Le développement rapide du cinquième domaine au cours des dernières décennies a révélé son rôle essentiel dans la géopolitique. Dans ce contexte, la Russie apparaît comme l'une des principales puissances du cyberespace, compte tenu de ses capacités comparativement plus avancées au niveau international. Ce document développe l'influence de la Russie dans le cyberespace dehors leurs frontières à travers deux cas. Le premier cas a lieu lors du plus important moment de la crise catalane en Espagne en 2017 et le deuxième concerne les élections françaises en 2017. On va découvrir à quel point les cyberattaques peuvent êtres perturbateurs même si elles n'atteignent pas leur objectif, et la nécessité de prendre des mesures pour les éviter.

MOTS CLÉS

La Russie, Cyber-attaque, désinformation, la Catalogne, la France.

Table des matières

Table des matières

Liste des figures et tableaux

1. INTRODUCTION

Dans un monde globalisé tel que celui dans lequel nous vivons aujourd'hui, nous ne pouvons pas ignorer l'évolution précipitée due au cyberespace et ses conséquences en matière de cybersécurité. Le développement rapide du cinquième domaine au cours des dernières décennies a révélé son rôle essentiel dans la géopolitique, en s'imposant comme un nouveau champ de bataille où les États Nations tentent de neutraliser les capacités économiques et militaires de leurs rivaux. Cela a été possible en raison des vulnérabilités et de l'inégalité dans les cyber-capacités des États (Kausch, 2018).

Le fait que l'utilisation mondiale de l'Internet ait augmenté à un taux de pourcentage supérieur à cent (Internet World Stats, 2020) a également déclenché une croissance de la cybercriminalité. Cela s'explique ainsi car il s'agit d'un crime de commission à faible risque avec des revenus substantiels (Fonfría & Duch-Brown, 2020).

En outre, la volatilité du cyberespace a entravé la capacité de la Communauté Internationale à légiférer conjointement dans ce domaine, entraînant des coûts économiques superflus, compte tenu du fait que la mondialisation et l'interdépendance multiplient les effets négatifs des cyberattaques, qui touchent le monde entier (Fonfría & Duch-Brown, 2020). De plus, l'utilisation de *proxies* lors de cyberattaques non seulement dans le cas de la Russie mais partout dans le monde, rend l'identification des auteurs très difficile (Baezner, 2018). En conséquence, l'impunité est même « favorisée » (Lewis, 2018).

Autrement dit, selon Ross Smith (2018), *« lorsque le système international devient progressivement plus multipolaire et moins ordonné, on se demande inévitablement dans quelle mesure il est possible de parvenir à une compréhension généralisable de la politique internationale »*. Cela est d'autant plus vrai, bien que l'évaluation de l'intention des acteurs dans le cyberespace soit beaucoup plus complexe que celle d'un acte militaire conventionnel. De plus, lorsqu'un État n'est pas en mesure de connaître cette intention avec certitude, il supposera qu'il s'agit d'une attaque (Hennessey, 2017).

C'est pour toutes ces raisons qu'on se rend compte que la cybersécurité est un sujet de recherche très actuel et important. Être conscient du domaine numérique et de ses

éventuelles conséquences est essentiel pour mieux appréhender l'évolution des relations internationales. D'abord, nous présenterons le sujet de manière plus générale en essayant de l'expliquer avec la théorie du réalisme néoclassique ; et puis, nous l'examinerons plus en détail à travers deux études de cas.

Dans ce mouvement d'idées, nous expliquerons l'influence que les cyber-attaques russes ont pu avoir sur la scène politique en Espagne et en France. Nous nous intéresserons notamment au pic de la crise catalane en 2017 autour du référendum[1] du 1er octobre (ci-après dénommé 1-O) ; et en France, à l'ingérence constatée pendant les élections présidentielles en 2017. En effet, à travers cette hypothèse nous chercherons à démontrer que les actes de désinformation en provenance de la Russie ont saisi les faiblesses de leurs scènes politiques respectives et ont eu un impact perturbateur. Tout cela s'inscrit dans le concept théorique de la Nouvelle Doctrine Militaire Russe de 2014.

2. CADRE D'ANALYSE

2.1. Revue de la littérature

Au cours des dernières années, l'intérêt et l'importance du dilemme de la cybersécurité[2] ont augmenté de manière exponentielle. De ce fait, la cybersécurité est devenue un élément essentiel de la politique étrangère de certains États, comme la Russie -une des principales cyberpuissances du monde- (Baezner, 2018) comme nous le constaterons au cours de cette analyse.

Avant d'analyser davantage la question qui nous occupe, nous allons donner un bref aperçu sur le domaine de la cybersécurité en Russie. En effet, le Kremlin part du principe que tout acteur perçu comme une menace ou un adversaire qui aurait pu un jour la mépriser, est susceptible d'être attaqué à tout moment (Greenberg, 2020). On doit être conscient du fait que le prochain essai portera sur deux cas concernant des cyberattaques

[1] Dans le présent document, la consultation des citoyens en date du 1er octobre sera appelée « référendum », compte tenu de son usage populaire. Toutefois, il convient de préciser qu'il ne s'agit pas de la terminologie correcte selon la législation espagnole (aux termes de l'Article 92 de la Constitution espagnole), car un référendum doit inclure l'ensemble des citoyens espagnols et non une région ; de ce fait, ceci a été caractérisé comme acte inconstitutionnel.

[2] Comprendre le dilemme de la sécurité dans une version cybernétique.

russes en 2017, lorsque les relations entre l'UE et la Russie se sont détériorées en raison de l'annexion de la Crimée (Milosevich, 2017 b). À partir de ce moment, l'hostilité russe envers l'Occident a été accentuée, tout comme le ton pro-Kremlinien des médias russes (Roman, Wanta & Buniak, 2017).

Tout d'abord, il est important de noter que la perspective de la Fédération Russe sur la cybersécurité diffère considérablement de celle de l'Occident. Alors que la première y voit un outil essentiel de politique étrangère et un moyen de protection d'intérêts politiques, culturels, économiques et militaires ; la seconde peine même à contrôler les cyberattaques étrangères (Kshetri, 2016). Par contre, concernant la prépondérance de l'offensive, la difficile traçabilité, l'escalade et le secret, les deux s'accordent (Medvedev, 2015).

En outre, il existe une grande ignorance généralisée par rapport à la réelle cybercapacité russe (Martínez Jiménez, 2015). De fait, il est possible que les plus récents logiciels malveillants actuellement utilisés par la Russie déclenchent une course aux cyberarmes au sein de la communauté internationale, notamment parmi les pays les plus vulnérables aux frappes russes (Baezner, 2018).

De plus, les Russes ont évidemment profité des moments de crise en Europe comme la crise économique en 2008 ou la crise migratoire en 2014, pour la cyberattaquer. C'est dans ces moments de tension que les attitudes eurosceptiques se développent et sont souvent réticentes aux changements politiques majeurs (Snegovaya, 2021). Selon les mots de certains chercheurs comme Hill (2021), pour la Russie « *the fire was already burning ; all Putin had to do was pour on some gasoline* ». Cette expression prendra corps tout au long de ce travail, étant donné que nous soutenons que les faiblesses structurelles d'un État, c'est-à-dire, qu'elles (pré)existent déjà ; sont exploitées par les cyberattaques russes.

Ainsi, il est important de comprendre d'emblée que les criminels, auteurs de cyberattaques agissent souvent avec l'accord du Kremlin, voire en tant qu'exécutants de la politique étrangère de la Russie. En effet, la relation entre *Russian Business Network* (désormais RBN) -l'un des groupes cybercriminels les plus connus opérant depuis le territoire russe- et le Kremlin a été prouvée (Kadlecová, 2018).

2.2. Théorie du réalisme néoclassique

La théorie qui explique le mieux le comportement de la Russie sur la scène internationale est le réalisme, en particulier le réalisme néoclassique[3] qui a émergé dans les années 1990. Le terme réalisme néoclassique a été introduit en 1998 par Gideon Rose comme une nouvelle approche à l'étude des relations internationales. Nous allons ensuite expliquer brièvement les principaux éléments du réalisme néoclassique, puis nous développerons la raison pour laquelle il correspond à la manière dont la Russie agit dans la communauté internationale.

D'une part, la tradition néo-réaliste a été maintenue en ce qui concerne l'influence des pressions provenant du système international (« pressions systématiques ») sur la politique étrangère d'un pays ; en la façonnant comme elle l'entend (Firoozabadi & Ashkezari, 2016). Preuve en est que, les cyberattaques visant l'Europe se sont considérablement intensifiées après l'imposition des sanctions économiques résultant de l'annexion de la Crimée par la Russie en 2014 (Milosevich, 2017 b). D'autre part, il introduit l'idée que le comportement des États sur la scène internationale est également influencé par des circonstances internes telles que les intérêts des acteurs nationaux (Firoozabadi & Ashkezari, 2016).

Dès lors, le réalisme néoclassique se positionne souvent quelque part entre la théorie réaliste et libérale. Cependant, c'est l'influence dominante des facteurs exogènes (« systémiques ») sur les facteurs nationaux qui éloigne un pays de cette logique de la théorisation libéraliste. Les facteurs externes apparaîtraient comme la variable indépendante, les facteurs internes comme la variable intervenante et la politique étrangère de l'État russe comme la variable dépendante (Romanova, 2012).

En tant que sous-catégorie du réalisme, le réalisme néoclassique repose sur l'idée que les États sont souverains et représentent donc les principaux acteurs des relations internationales. Cependant, contrairement au réalisme classique, qui se concentre sur les

[3] Malgré le fait que la personne de Vladimir Poutine ait été associée à la théorie réaliste par des institutions telles que l'Institut Français des Relations Internationales (Lo, 2018).

facteurs internes et humains, le réalisme néoclassique prend en compte la structure du système international et analyse son impact sur le comportement des États (Joseph, 2014).

En outre, il se préoccupe principalement de la sécurité de l'État. Il contiendra donc les politiques que l'État (en l'occurrence de la Russie) adopte lui-même pour protéger sa sécurité. Les réalistes néoclassiques interpréteront les pressions provenant du système international (« pressions systémiques ») et, sur cette base, élaboreront la politique étrangère qui conviendra le mieux à l'État (Firoozabadi & Ashkezari, 2016). À cet égard, il convient de noter que les tensions dans les relations entre la Russie et l'UE qui ont suivies l'annexion de la Crimée en 2014 ont marqué un tournant. Par conséquent, ce n'est pas une coïncidence si la Nouvelle Doctrine Militaire de la Fédération Russe, que nous allons décrire ci-dessous, a été adoptée en 2014.

Si on analyse d'une façon plus pratique pourquoi l'esprit de la Russie est hautement réaliste néoclassique, on doit se centrer sur deux éléments :

a. Un grand (historiquement) pouvoir de l'État central avec un leader fort comme Poutine dans les vingt dernières années, qui place l'État et ses intérêts au centre de l'élaboration de la politique étrangère (Wieclawski, 2011).
b. L'instrumentalisation des intérêts nationaux afin de légitimer le comportement de l'État et gagner le soutien de l'opinion publique et de l'élite russe. En effet, faire passer les intérêts nationaux avant les valeurs est une caractéristique de la politique étrangère russe[4] (Romanova, 2012).

Si on examine de près ces deux points, nous constatons qu'au final, l'objectif de la Russie est de retrouver son statut de superpuissance dans le monde, de « se faire respecter » (Pavlova & Romanova, 2012). Par conséquent, ses efforts pour générer le chaos en Occident ne sont pas vains. D'un côté, ils veulent être traités d'égal à égal à la table des négociations au niveau international[5]. D'un autre côté, ils peuvent justifier les tendances autocratiques de Poutine (Krah, 2021). Après tout, « l'anti-occidentalisme » est l'un des piliers du régime russe (Milosevich, 2017 b).

[4] Quelques auteurs comme Romanova (2012) considèrent que cette forme de comportement sur la scène internationale est une réponse à la concurrence idéologique de l'Occident.

[5] Néanmoins, cela ne risque pas d'arriver à moyen ou long terme de sorte que ces attaques ne cesseront pas de sitôt non plus

2.3. Problématique

Les efforts inlassables de la Fédération Russe pour poursuivre les cyberattaques perturbatrices et délétères ont pour but d'étaler ses capacités et d'envoyer des messages hautains au monde, soulignant sa grandeur (Baezner, 2018). Etant donné que nous évoluons dans « *un monde où cliquer sur le mauvais lien ou négliger un simple correctif logiciel peut entraîner un incident géopolitique* », les efforts de la Russie pour exploiter les faiblesses de ses voisins européens sont facilités (Inglis & Krejsa 2022, par. 10).

Les crises antérieures qui ont frappé l'Europe[6] (crise économique de 2008, Brexit, crise migratoire de 2011, attentats terroristes islamiques...) ont mis en évidence la fragilité du système libéral, permettant ainsi à la Russie d'atteindre ses cibles plus facilement dans la guerre de l'information. Cela signifie qu'il leur a été plus simple de créer une perception déformée de la situation politique dans les pays occidentaux, avec toutes les conséquences que cela implique. Celles-ci seront analysées plus avant (Milosevich-Juaristi, 2017 a). En outre, personne ne peut garantir que les cyberattaques ne se reproduiront pas, ce qui met constamment en péril la pérennité de la démocratie (Pally, 2020).

Les acteurs de la scène internationale, comme la Fédération Russe, profitent des faiblesses présentes dans les réseaux sociaux, couplées à la franchise des citoyens, ce qui donne lieu à ce que beaucoup appellent « l'armement du big data ». Grâce à ces outils, la polarisation dans les débats sensibles tels que l'immigration, la religion ou le genre est inévitable. Nous devrions alors être conscients d'une éventuelle ingérence extérieure, car elle peut manipuler le jugement des citoyens (compris comme citoyens d'États démocratiques occidentaux), et réorienter le cours politique d'un État (Polyakova & Boyer, 2018).

Pour ce faire, la Doctrine Militaire de la Fédération Russe (2014) fixe comme objectif principal de ne pas détruire l'ennemi, mais de l'influencer et de le guider vers son propre déclin. À cette fin, elle a recours à des armes non conventionnelles, telles que la (dés)information ou la guerre psychologique ; dans le but ultime de rendre à la Russie son statut de grande puissance (Milosevich-Juaristi, 2017 b). En résumé, l'utilisation de campagnes de désinformation, de *proxies*, de cyberattaques, etc. vise à déstabiliser

[6] Considéré dans ce document comme un bloc culturel/idéologique, inclus dans l'Occident.

l'Occident et à tromper les sociétés démocratiques, à affaiblir les institutions européennes et à entraver les accords transatlantiques (Polyakova & Boyer, 2018). En effet, selon les mots de l'ancien procureur général adjoint des États-Unis, John Demers « *no country has weaponized its cyber capabilities as maliciously or irresponsibly as Russia, wantonly causing unprecedented damage to pursue small tactical advantages and to satisfy fits of spite* » (in Greenberg 2020, pár. 4).

Même si ces actions ont été perpétuées au cours de la dernière décennie dans toute la civilisation occidentale (Snegovaya, 2021), on limitera l'analyse dans ce travail à deux cas : la cyber-activité russe au plus haut de la crise catalane en 2017 et lors des élections françaises de 2017.

Un autre problème majeur dans ce domaine (souligné par des experts comme Buchanan), est la difficulté pour la cybersécurité d'identifier la véritable intention derrière une attaque dans le cyberespace, en comparaison à l'arène militaire conventionnelle, où le dessein est clair. Ce flou empêchera l'État victime de se défendre en connaissance de cause (Hennessey, 2017).

Pour clore la question, il serait utile de clarifier les trois mécanismes utilisés par la Russie pour manipuler l'opinion publique dans les études de cas qui seront détaillées ci-dessous :

1) **Les médias contrôlés par l'État russe :** Les plus connus sont RT, Sputnik et Russia Beyond the Headlines. Principales sources d'information des russes, elles sont utilisées pour manipuler leurs propres citoyens à l'intérieur de leurs frontières. À l'étranger, certaines comme RT sont considérées comme les plus grandes organisations de l'économie politique mondiale de la désinformation (Krah, 2021). À titre d'exemple, dans le cas de la Catalogne, Sputnik et RT étaient les plus grands fournisseurs de (dés)informations (Lesaca, 2017).

2) **Les opérateurs et les cyber opérations** : Ces termes comprennent principalement la collecte illégale d'informations et sa diffusion ultérieure déformée. Il convient de préciser que ces opérations de cyberespionnage ne pourraient avoir lieu sans la collaboration d'opérateurs privés, mieux connus sous le nom de *whistleblowers*. Parmi les personnes les plus emblématiques figurent

Julian Assange et Edward Snowden, dont les liens avec le Kremlin n'ont pas été formellement prouvés malgré les soupçons internationaux (Krah, 2021).

3) **Les réseaux sociaux** : Comme les deux précédents, les réseaux sociaux ont été utilisés pour influencer politiquement d'autres États et diffuser de faux messages. De plus, ce genre d'activité est normalement utilisée au moment qui précède ou qui suit immédiatement un événement clé au plus fort d'une crise (Krah, 2021). De cette façon, la Fédération Russe a utilisé des *trolls,* des *bots* et des *cyborgs*. D'une part, les *trolls* sont des personnes qui créent de faux profils et/ou blogs sur Internet afin d'envahir la toile de fausses nouvelles, illusoires ou pro-Kremlin ; et en contrepartie, ils reçoivent une récompense financière. D'autre part, les *bots* sont utilisés pour amplifier la diffusion d'informations de manière automatique et systématique, généralement par l'utilisation de faux profils sur les réseaux sociaux. Les bots peuvent être classés comme bénins (ceux qui partagent des informations et des nouvelles réelles) ou malins (ceux qui diffusent du contenu malveillant et du spam). Les *cyborgs*, quant à eux, ont une nature à mi-chemin entre l'humain et le robot. En d'autres termes, il peut s'agir d'un robot assisté par un humain et vice versa (Chu, Gianvecchio, Wang & Jajodia, 2010).

   L'essor étonnant des médias sociaux au cours de la dernière décennie ne laisse aucun doute sur l'influence qu'ils exercent sur la population. En outre, ils constituent un facteur majeur de polarisation et de déstabilisation des démocraties libérales modernes (Iosifidis & Wheeler, 2018) ; une autre raison pour laquelle la Russie s'en servirait.

2.4. Justification choix des pays

Par rapport aux pays choisis pour ce mémoire, on peut dire que l'Espagne et la France, bien qu'ils soient géographiquement adjacents et à l'ouest de l'Europe, ont des systèmes politiques bien différents. Pour rappel, la France est l'un des pays les plus centralisés du monde, contrairement au modèle espagnol, décentralisé et proche du fédéralisme. Les deux États comprennent d'anciennes civilisations qui ont modelé au cours de l'histoire la pensée occidentale et fondé des valeurs traditionnelles telles que le christianisme (Pasquier, 2004).

Ensuite, on se référera brièvement aux principaux défis et faiblesses auxquelles leurs systèmes politiques respectifs font face, et qui par ce fait constituent la cible des cyber-attaques russes[7].

Dans ce sens, l'un des plus grands défis pour l'Espagne est sans aucun doute le sécessionnisme catalan. À cet égard, il faut savoir que l'immense degré de décentralisation attendu par certaines communautés autonomes comme la Catalogne, n'a pas conduit à l'atténuation des revendications souverainistes, y compris celles de l'opinion publique (Vilanova, 2008). Cette difficulté structurelle ne passe pas inaperçue auprès d'acteurs tels que la Russie, qui, suivant la logique (néo)réaliste, saisissent chaque opportunité pour faire de la scène internationale la cible de ses intérêts nationaux (Romanova, 2012).

Il y a également d'autres problèmes structurels qui entravent la gérance de l'État. Par exemple, certains acteurs politiques et sociaux ont proposé des tentatives sérieuses de révision de la transition et de la démocratie espagnole en général (Vilanova, 2008). Par conséquent, ce n'est pas surprenant que les parties les plus révisionnistes et extrêmes espagnols soient ceux qui aient les liens les plus solides avec le Kremlin[8] (Casal, 2022). Par ailleurs, la croissance exponentielle de l'influence des médias sur la population a encouragé la proximité entre les médias et les partis politiques espagnols. Cela a favorisé la polarisation, résultat de l'affrontement entre les différents moyens de communication (Vilanova, 2008). De fait, l'utilisation des médias par le Kremlin pour « révolutionner » les populations occidentales est bien connu comme nous l'expliquerons ci-dessous.

En consultant de grandes collections historiques, on remarque que la France a été pionnière en matière de droits humains, valeur qui couronne l'identité occidentale et donc européenne (Soutou, 2004). Compte tenu de cela, il est évident que l'orientation que prendra la direction politique de la France aura inexorablement un effet majeur sur la scène européenne. Sa place dans le monde, les intérêts qu'elle souhaite défendre, les valeurs qu'elle veut promouvoir… sont des questions dont la réponse change énormément en fonction de l'administration du moment (Faure & Boyon, 2006). De ce fait, une éventuelle ingérence dans les élections françaises peut être vue comme une importante

[7] Compte tenu des limitations de ce travail de recherche et de l'existence de plusieurs facteurs.
[8] Doit être pris en compte dans les moments précédant l'invasion russe de l'Ukraine.

attaque contre la démocratie, non seulement française mais également européenne. L'effet d'une telle attaque en France aurait plus d'impact au niveau international, en particulier européen, que si elle était dirigée contre un autre pays.

2.5. Question de recherche

La question de recherche sera la suivante : dans quelle mesure les cyber-attaques russes ont-elles influencé la scène politique en Espagne au plus fort de la crise catalane en 2017 et en France lors des élections de 2017 ? Pour y répondre, nous analyserons l'impact des manœuvres *ultra vires* de la Russie sur ces deux États d'Europe du Sud et nous exposerons les raisons et les intérêts que sous-tendent ces cyber-attaques. Tout cela confirme l'arrivée imminente du cinquième domaine de la guerre, le domaine numérique (Polyakova & Boyer, 2018).

D'un point de vue plus technique, il convient de clarifier que la variable indépendante sera celle des cyber-attaques russes et la variable dépendante sera l'influence sur les deux États proposés de l'Europe de l'Ouest. Bien que l'impact comparatif de la (cyber)Russie sur les politiques respectives des deux pays ne soit pas exactement parallèle, il vise plutôt à affaiblir l'UE et son modèle d'organisation. Afin de clarifier la portée des deux variables, une brève explication des termes mentionnés dans la question recherche est donnée ci-après.

Premièrement, les *cyber-attaques* russes doivent être comprises comme *« la diffusion d'informations défavorables ou trompeuses sur des institutions et des gouvernements étrangers par le biais de fuites de documents souvent obtenus par piratage, harponnage ou autres formes d'espionnage »* (Connel & Vogler 2016, p.17). Cette dissémination de données a été réalisée par trois moyens : les médias contrôlés par l'État russe, les opérateurs et les cyber opérations, et les réseaux sociaux ; en ayant un effet perturbateur sur les États respectifs (Krah, 2021). À cet égard, il faut comprendre que dans le cyberespace, un outil essentiel est la *représentation*. La construction particulière qu'on fait de la réalité, même si elle garde un lien évident avec les faits objectifs, maintient inexorablement un caractère subjectif. Cette subjectivité est ce qu'on lie à la dénommée *représentation*. De cette façon, les *représentations* ne sont pas neutres, mais elles

convainquent, mobilisent, polarisent ou inquiètent leurs cibles selon une stratégie concrète (Douzet 2014, p. 8).

Par rapport à ce que l'on entend par le mot *influence* (compte tenu de sa subjectivité possible également), il s'agit surtout de la perturbation et du bouleversement, causés par le climat politique de l'État concerné. Cela contribue aussi à la tension et à la polarisation de la société (Iosifidis & Wheeler, 2018). Cela nous amène au point suivant : qu'entendons-nous par *tension* ? Selon Larousse, le mot *tension* implique un « état (…) qui est tendu, contracté, nerveux » ou même une « situation tendue entre deux groupes, deux personnes, deux États ».

Dans le cas de l'Espagne, il y avait clairement une opposition importante entre deux groupes ou deux discours opposés : les indépendantistes versus les non-indépendantistes. Ce désaccord a créé une situation tendue non seulement dans la région catalane mais aussi dans la totalité du territoire national. En France, la confrontation était plutôt idéologique. Les pensées en question étaient celles proposées par les partis politiques dont les intentions de vote étaient les plus élevées à l'époque précédant les élections : celles du parti Rassemblement National et celles du parti La République en Marche[9]. Parmi les sujets les plus controversés figure la question de l'appartenance de la France à l'UE (Rassemblement National, 2017).

Si on met les deux cas en parallèle, on voit que les cyber-attaques perpétrées en Espagne ont eu plus de succès en termes de ciblage : le climat de polarisation, la déstabilisation de l'État central (avec la crise politique qui s'est déclenchée après) et le sentiment de malaise des citoyens face à cette crise ; ont été accentués pendant la période de pointe de la cyberactivité russe -bien que la Russie n'ait pas été responsable de ces phénomènes-. Par ailleurs, en France, bien qu'elle ait eu un impact éphémère sur la fluctuation des intentions de vote avant les élections, les résultats de celles-ci n'en ont pas été affectés. En fait, le candidat lésé par les cyber-attaques était le vainqueur de l'élection : Macron. En somme, malgré les effets minimaux qui pourraient être liés à la Russie, nous constatons un échec à court terme des cyber-attaques dans les deux cas. Cependant, la question se pose de son

[9] Ayant récemment changé de nom pour devenir *Renaissance* (AFP, 2022).

éventuel impact à long terme (Kamiya, Kang, Kim, Milidonis & Stulz, 2018), notamment en ce qui concerne la croissance de l'extrême droite en Europe.

Finalement, pour déterminer le rôle des scènes politiques dont il est question, nous le circonscrirons à l'atteinte à la réputation démocratique et à la polarisation des citoyens en Espagne ; ainsi qu'à la fluctuation des intentions de vote dans le cas de la France. Dans ce cadre, il est intéressant de souligner l'existence d'une polarisation émotionnelle dans les deux cas qui entraîne « une division résultant d'un manque de respect pour ceux qui défendent des positions différentes de leur propre » (Barbet 2020, p.7).

2.5. Hypothèses envisagées

Dans ce mémoire, le but principal est de vérifier l'hypothèse proposée, à savoir : « *les cyber-attaques ciblent dans des moments de grande tension et renforcent les faiblesses structurelles dans ces pays-là* ». Etant donné que nous avons choisi deux pays de l'Europe de l'Ouest, l'Espagne et la France, on essayera de prouver que leurs faiblesses respectives ont été exploitées par les cyber-attaques russes. En effet, nous défendrons que la manière et le moment d'agir n'ont pas été choisis de façon anodine, mais dans un but explicite de chaos et d'instabilité.

Dans le cas de l'Espagne, la Russie a tiré profit de l'absence d'un sentiment d'appartenance dans certaines régions, à savoir, la Catalogne. De cette façon, la polarisation de la totalité de la population espagnole a été inévitable, non seulement en raison des cyber-attaques mais aussi d'autres facteurs comme la presse nationale (Masip, Suau & Ruiz-Caballero, 2020). Par contre, en France, en considérant le climat de radicalisation politique et le mécontentement au sein de la société française -leurs faiblesses-, (Boelaert, Michon & Ollion, 2018) les cyber-attaques ont été perpétrées dans le but de voir le parti radical arriver au pouvoir (Pocheptsov, 2017).

De fait, selon certaines expertes comme Polyakova (2017), les cyber-attaques russes devraient être cadrées dans un contexte beaucoup plus global, visant à la désintégration de l'Europe. En diffusant les idées pro-Kremlin dans l'UE -qui sont clairement en contradiction avec celles de l'Occident-, ils « amèneront les gens à s'interroger sur les fondements des systèmes dans lesquels ils vivent » (Thoburn en Dorell, 2017). À cette

fin, ils ont encouragé des acteurs et/ou des actions qui favorisent leurs intérêts dans les deux États étudiés, comme on le verra plus loin.

Enfin, il faudrait préciser ce que nous entendons par « désintégration de l'Europe ». Bien qu'elle puisse être comprise de manière plus abstraite comme « civilisation », nous le limiterons au niveau de l'UE. Dans ce sens, le déclin de l'UE -en tant qu'institution modèle pour le monde entier- pourrait être motivé par des événements tels que le *Brexit* ou les désaccords survenus en son sein en raison de divergences d'opinion sur la position internationale[10] qu'elle a adoptée. Il convient également de préciser qu'une perturbation dans l'un ou l'autre des États membres de l'UE entraînera à terme une perturbation de l'UE dans son ensemble. C'est pourquoi les deux États proposés, la France et l'Espagne, font partie de la stratégie de cyber-attaque contre l'UE.

Concernant les effets spécifiques causés par l'ingérence russe à l'intérieur des États concernés, nous pouvons dire ce qui suit. D'une part, pour la France, l'intervention russe avait pour but le sabotage de Emmanuel Macron lors de l'élection présidentielle de 2017, au profit du parti extrémiste de Marine le Pen, qui est plus aligné sur certaines idées du Kremlin (Chausovsky, 2018). D'autre part, l'Espagne a été affectée par l'infiltration de la Russie dans le contexte de la crise catalane en Espagne et la diffusion de fausses informations sur la tenue du référendum en Catalogne en 2017. Ce fait a attisé le climat de crise et endommagé l'image d'un pays démocratique comme l'Espagne (David, 2018) ; malgré ses effets limités dans le temps.

Quant à la méthodologie de ce travail, l'étude de cas sera utilisée. De cette manière, on prouvera l'hypothèse proposée à travers deux cas différents, à savoir l'Espagne et la France, victimes de cyber-attaques similaires. Grâce aux événements décrits dans ces deux cas et les conséquences que nous pouvons raisonnablement présumer être le résultat de la cyber-activité russe, nous parviendrons à certains parallélismes, différences et conclusions entre les deux situations. En tout cas, l'ingérence sur les scènes politiques de l'Espagne et de la France a profité de leurs faiblesses respectives.

[10] La controverse sur la construction du gazoduc Nordstream 2 en est un bon exemple : de nombreux députés européens ont fait valoir que ce projet d'ingénierie violait la politique commune de sécurité énergétique de l'UE (Parlement Européen, 2021).

Concernant la recherche d'informations, la plupart sont extraites d'articles scientifiques. Néanmoins, les articles de presse de 2017 ont aussi été une source importante pour évaluer l'environnement dans les moments où les événements se déroulaient. En outre, l'utilisation de l'interview -transcrite en annexe- a été fondamentale pour pouvoir tirer une véritable conclusion et réfléchir à la manière de prévenir ce type d'actions perturbatrices.

3. LA CRISE CATALANE EN ESPAGNE EN 2017

3.1. Présentation de faiblesses-cible en Espagne

La complexité territoriale et identitaire « centre-périphérie » qui caractérise l'Espagne est clairement un trait distinctif de son système politique, qui n'est pas passé inaperçu auprès de la Russie. Par exemple, malgré le principe de *shared rule* qui guide a priori l'organisation de pouvoir, la région catalane a développé une voie indirecte de pouvoir dans le gouvernement de l'État. De cette façon, il y a sur place un système de pouvoir imparfait qui contribue à consolider une asymétrie informelle entre certaines régions espagnoles, la Catalogne étant l'une des plus puissantes (Pasquier, 2004). En effet, l'Espagne est, avec la Belgique, l'un des pays qui a le plus décentralisé sa structure étatique au cours des cinquante dernières années (RIE, 2019).

Concernant le conflit catalan en particulier, l'origine remonte à plusieurs siècles. Ce qui explique que sa situation soit si complexe et que sa nature soit clairement structurelle. Au niveau historique, l'Espagne a été paradoxalement caractérisée par le maintien de l'intégrité territoriale et les tensions de pouvoir et d'identité. Dans cette logique, il est important de mentionner que la création précoce de son État ne s'est pas accompagnée de la construction d'une nation moderne, qui ne s'est ajoutée qu'au XIXe siècle. En d'autres mots, la mise en place de l'État dit moderne, qui a eu lieu au XVe siècle, n'a pris en compte que partiellement les identités, et s'est davantage concentré sur l'homogénéisation religieuse. De même, le Royaume de Castille, dont la langue est majoritaire, prendra la tête de ce processus. Ce processus d'homogénéisation voulu et long n'a jamais été achevé, car la concurrence des identités ne l'a pas permis (RIE, 2019).

Si nous mettons à jour la question catalane, elle s'explique généralement par ce que l'on appelle la « triple crise », économique, politique et territoriale, qui a contribué à

l'exacerbation du conflit ces dernières années. Premièrement, la crise financière de 2008 qui a frappé le monde entier, a eu un impact particulièrement négatif en Espagne au niveau économique, et causé un rejet ultérieur de la région catalane envers le gouvernement de Madrid. Deuxièmement, la crise politique a été un résultat de l'épuisement des accords de la Transition et de la sclérose partisane » entre les deux principaux partis et leur corruption. Cela a conduit à l'apathie des citoyens, notamment des catalans. Troisièmement, l'affaiblissement du modèle territorial qui est né avec la Constitution de 1978, et qui répondait aux demandes d'autonomie de régions comme la Catalogne, n'est plus suffisant (Serra, Ubasart & Martí 2018, pár. 4).

D'un point de vue plus « social », les citoyens eux-mêmes l'ont fait savoir à travers l'enquête sociale européenne 2017-2018 ; où ils ont déclaré que ce pays tente depuis des années de faire cohabiter des identités différentes et des idéologies doubles qui ne se rejoignent pas tout à fait (Silvestre, 2020). Ce sentiment de ne pas « être à sa place », ou de ne pas s'identifier à l'identité centrale de l'État, peut être exacerbé dans les moments de tensions comme le 1-O. Si nous nous référons à la définition de *tension* de Larousse, cela nous parle d' une situation « tendue ou nerveuse » ou même d'un affrontement entre « deux groupes ou deux États ». C'est pourquoi, un référendum pour décider de l'intégrité territoriale d'un État ou de la création d'un nouvel État au XXIe siècle, constitue clairement un contexte de *tension*.

Dans ce cadre, l'état d'étroitesse et de malaise liés à l'incertitude de ces jours vécus aux alentours du 1-O, prédispose les citoyens à être « surinformés » ; ce qui facilite la consommation de *fake news* et de désinformation. Dans de telles situations, le monde virtuel est un moyen parfait pour promouvoir le flou et la confusion, et en même temps l'exploitation par des acteurs tels que la Russie pour alimenter la polarisation. Ce qui nous amène au point suivant : les perceptions. Les médias comme Twitter, ont été utilisés comme booster pour donner au public le sentiment erroné d'une polarisation incontrôlée. Ce n'était pas forcément le cas, mais c'est vrai que les personnes les plus manichéennes et les plus polarisées par rapport au conflit catalan, étaient plus disposées à être présentes sur les réseaux sociaux (Barbet, 2020).

Ceci étant dit, l'ultra-activité de certains comptes pro-indépendants provenant de la Russie ont favorisé cette perception. En somme, la cyber-activité russe a provoqué des

perceptions de polarisation et entravé la résolution de la crise. Néanmoins, la réputation de l'Espagne n'a pas été aussi endommagée comme les cyber-attaques l'ont prétendu.

3.2. Raisons de la Russie

Par rapport aux motivations du Kremlin pour un tel comportement, la logique néo-réaliste est d'une grande aide pour mieux comprendre. En effet, si on se demande pourquoi un État aussi grand que la Russie décide d'intervenir dans les affaires intérieures d'un autre État qui a historiquement entretenu de bonnes relations avec elle -par rapport à d'autres États-, (Rankin, 2017) on arrive aux conclusions suivantes.

Après tout, l'anti-occidentalisme est l'un des piliers de la pensée russe[11] (Milosevich, 2017 b), et tout dysfonctionnement au sein de l'UE ou des valeurs libérales proposées par l'Occident sera considéré comme une victoire par la Russie. De cette façon, si la Catalogne se séparait de l'Espagne, cela contribuerait à prouver « leur point de vue » : le projet de l'UE est voué à l'échec et son démembrement est inévitable. À cet égard, on observe sa logique néo-réaliste : d'un côté l'État-nation traditionnel a la priorité en tant que souverain sur toute organisation (Joseph, 2014) ; et d'un autre côté, le comportement externe de l'État est influencé par des intérêts internes (Firoozabadi & Ashkezari, 2016).

Par ailleurs, leur sympathie pour l'indépendantisme catalane a aussi été mis en parallèle avec le soutien russe aux régions d'Abkhazie et d'Ossétie du Sud en Géorgie et sa déclaration unilatérale d'indépendance (Alandete, 2017 b). Compte tenu de ces actions, on peut apprécier une certaine philosophie de « l'ennemi de mon ennemi est mon ami ». Dans ce cadre, une région comme la Catalogne, qui remet en question le statu quo dans un pays de l'UE et ergo de l'UE elle-même, va donc obtenir la bénédiction de la Russie.

Ceci étant dit, en ce qui concerne la respectabilité de l'État espagnol à l'étranger, les cyber-attaques ont échoué à court terme. Malgré l'alarme initiale internationale concernant les événements du 1-O et les difficultés rencontrées par l'État espagnol dans la gestion de la crise -alimentées par les cyber-attaques russes- ; l'objectif n'a pas été atteint. Du fait, comme nous le verrons plus loin, les institutions européennes et tous les

[11] Compris comme les valeurs défendues par le Kremlin.

dirigeants internationaux se sont positionnés en faveur de l'intégrité territoriale de l'Espagne et ont manifesté leur soutien au gouvernement central (Molina & Martín, 2019).

3.3. Événements

Cette section décrira les principaux événements près du 1-O qui ont vraisemblablement été réalisés par le Kremlin.

D'abord, il est important de savoir au préalable que les « cyber-armées » du Kremlin ont diffusé des informations et des messages faux et/ou biaisés afin d'exacerber la crise et de polariser la société, non seulement en Espagne mais aussi à l'étranger. Du fait, les autorités espagnoles de l'époque n'ont pas hésité à en parler publiquement de ces manœuvres, en les associant directement avec l'État russe -même si ce dernier a nié ces accusations dans ses propres articles- (Emmott, 2017).

En pleine crise, les actions malveillantes les plus représentatives promues par la Fédération Russe sont la propagation d'informations frappantes à travers leur média nationaux RT et Sputnik, et sa diffusion massive à travers les réseaux sociaux Twitter et Facebook -même si les informations promues par la presse et les médias sociaux se chevauchent souvent-.

3.3.1. Médias russes: RT et Sputnik

Par rappel, deux des plus importants médias financés par l'État russe, à savoir RT et Sputnik, sont parmi celles qui ont les plus publié sur le conflit catalan. En effet, le contenu partagé par RT et Sputnik, a été dix fois plus élevé que les informations fournies par les médias officiels publics espagnols tels que RTVE[12] (Radio Televisión Española) ou Agencia EFE (Lesaca, 2017).

[12] Radio Televisión Española est le fournisseur d'informations de l'État par excellence, étant une société entièrement détenue par l'État. Elle gère indirectement le Service public de radio et de télévision en Espagne (RTVE).

Les références qui ont été faites concernant la crise catalane, affirmaient qu'une guerre civile était sur le point d'éclater en Espagne -en la comparant à Donbass en Ukraine- et que la violence exercée par les forces de sécurité de l'État était typique de la dictature de Franco et non d'un État démocratique soumis à l'État de Droit. Ils ont également assuré que l'UE reconnaîtrait la Catalogne comme un État indépendant après avoir suivi le processus d'adhésion (Milosevich 2017 b).

En plus, si on examine de plus près les dix nouvelles les plus partagées par ces médias, nous constatons que leur intérêt principal était de souligner la présence de violence dans les événements. Les chiffres qui suivent, correspondant à RT, montrent plus spécifiquement les pourcentages : 50 % ont dénoncé le comportement de la police espagnole, 10 % ont remarqué les dommages économiques que l'indépendance de la Catalogne apporterait à l'État espagnol, 20 % sont restés neutres et 10 % ont critiqué le président espagnol du moment, Mariano Rajoy. En bref, les médias russes ont mis l'accent sur les éléments les plus négatifs et nuisibles (Palmer, 2017).

Par contre, si nous nous arrêtons pour analyser la véracité de ces communications, nous découvrons sa nature de *fake news*. À titre d'exemple, l'Espagne n'a jamais été dans ces jours-là au bord du conflit armé. Également, on constate qu'il serait imprécis d'affirmer que l'UE admettrait volontiers la Catalogne en tant qu'État indépendant même si le processus d'adhésion était suivi. Cela s'explique par le fait qu'un vote unanime des membres de l'UE serait nécessaire -y inclus celui de l'Espagne-, ce qui est peu probable dans ces circonstances (Molina & Martín, 2019).

En outre, plusieurs photos partagées dans les susmentionnés comptes, ne correspondaient pas aux événements du 1-O, c'est-à-dire, elles ont été prises à partir d'un autre incident, se faisant passer pour des vraies images du 1-O (BBC Mundo, 2017).

Enfin, le pire dans toute cette affaire est que la diffusion massive de ces (dés)informations, a eu lieu par moyen des *bots* et des *trolls* en retweetant dans les réseaux sociaux de manière incontrôlée et hyperbolique (Milosevich, 2017 b), comme on le verra dans la sous-section suivante.

3.3.2. Réseaux sociaux: Twitter

Les communications provenant des réseaux sociaux se sont surtout diffusées à partir des comptes de sympathisants du Kremlin tels que Julian Assange et Edward Snowden. À cet égard, il faut souligner que Sputnik a beaucoup insisté sur les tweets publiés par Assange -même avant le référendum- au détriment des autres comptes y inclus ceux du gouvernement de la Catalogne et de l'Espagne. D'autre part, Assange n'avait jamais publié sur l'affaire catalane jusqu'à septembre 2017, ce qui souligne que cette attention démesurée était due au fait qu'il critiquait délibérément l'État espagnol (Rankin, 2017). En effet, il a été prouvé que dans les jours précédents le référendum et pendant le 1-O lui-même, l'activité des *bots* d'origine russe a considérablement augmenté (Krah, 2021).

À titre d'exemple, dans l'image suivante, on trouve une preuve claire du biais présent dans la manière russe d'informer. Ce tweet du RT, est non seulement contraire au droit espagnol mais aussi faux, vu l'inconstitutionnalité du référendum et le faible taux de participation -inférieur à 50 %- (Statista Research Department, 2021).

Figure nº 1: Tweet de RT en 2017

RT (2017). *Twitter*. Last Retrieved on the 2nd of February 2022 from https://twitter.com/rt_com/status/914620944957759488?ref_src=twsrc%5Etfw

Une autre statistique étonnante démontre que seul le 9 % des comptes les plus actives, -partageant ces fausses nouvelles et provenant de RT ou de Sputnik- semblaient être de vraies personnes. En plus, quelques-uns de ces faux comptes partageaient environ 1.400 messages par jour inondant les réseaux (Lesaca, 2017). Encore une fois, on trouve la stratégie consistant à inonder le web de fausses nouvelles ou de nouvelles biaisées, afin de confondre l'opinion publique. En somme, dans cette section nous avons essayé de donner un aperçu des événements les plus significatifs concernant l'intromission de la Russie dans les jours précédant le 1-O.

3.4. Impact en Espagne

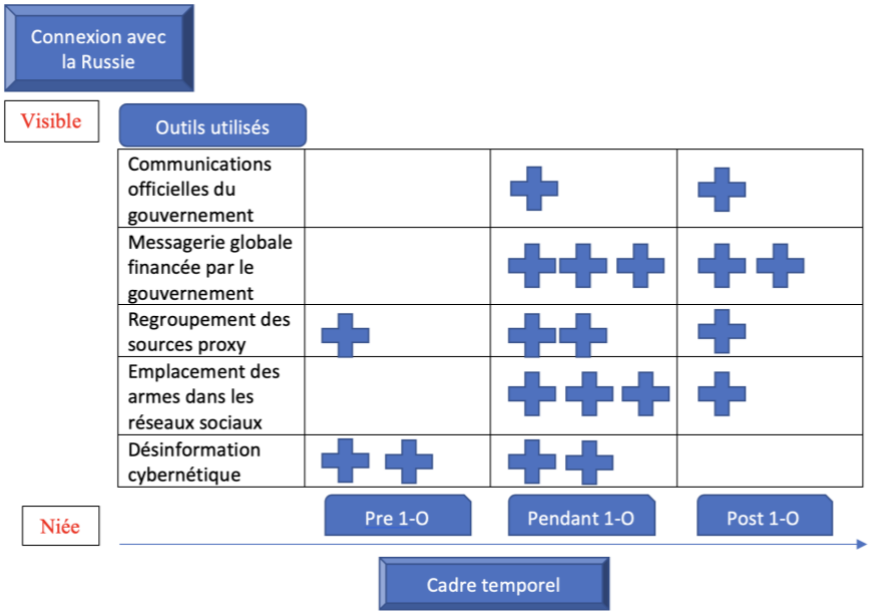
Si nous mettons en relation les actions décrites dans la section précédente avec les objectifs de la Russie, on constate l'existence de certains liens entre la cyberactivité et un léger changement de ce qu'on entend par la « scène politique » en Espagne. À titre de précision, l'impact sera mesuré à travers deux catégories : le dommage causé à la réputation de l'État espagnole et sa démocratie à l'étranger ; et l'alimentation de la polarisation de la société.

En ce qui concerne l'atteinte à l'image de l'Espagne à l'étranger, il est vrai que dans un premier temps, la réputation démocratique de l'Espagne a subi quelques dommages dus à un certain nombre de facteurs -parmi eux, la cyberactivité Russie-. Cependant, on ne peut pas conclure qu'elles étaient satisfaisantes, car cette première impression s'est rapidement améliorée et l'Espagne a reçu le plein soutien de l'UE. Par rapport à l'alimentation de la crise social, même si on observe une polarisation croissante et un soutien grandissant aux pro-indépendants en période de cyberactivité russe accrue ; la détente de la situation sociale a eu lieu rapidement. Cependant dans les deux cas, les cyber-attaques n'ont pas été les seuls facteurs à l'origine du résultat préconisé dans ce document. En somme, les cyber-attaques peuvent exacerber la polarisation ou les tensions déjà existantes, mais il est vraiment difficile de démontrer que cette polarisation est directement causée par une cyber-attaque particulière (Wolff, 2022).

3.4.1. Damage à la démocratie espagnole

Selon Milosevich (2017 b), l'un des objectifs principaux russes à atteindre en Espagne était le discrédit de sa démocratie. Ceux-ci ont donc promu une mauvaise presse des événements qui se sont déroulés le 1-O. Avant de procéder au développement de la mesure dans laquelle ce discrédit a eu lieu -sur la base des objectifs de la Fédération Russe- ; on va montrer à travers un tableau, la fluctuation de l'intensité de la cyberactivité de la Russie. À cet égard, on peut clairement voir que la désinformation promue par le Kremlin est plus grande avant et pendant le 1-O, détail qui influencera dans les résultats expliqués dans cette section.

Figure nº 2 : Tableau de différenciation des actions russes avant, pendant et après le référendum du 1-O -dont l'explication détaillée se trouve en annexe I-.



(Krah 2021, p. 53) - traduction

a) Discréditer la démocratie espagnole à l'étranger

Une partie de la presse internationale, y compris RT, a fait l'écho des épisodes de violence du 1-O en Catalogne et a présenté l'Espagne comme un État répressif, voire a favorisé la vision pro-indépendance. Il ne fait aucun doute que ce n'est pas le seul facteur qui a nui

à l'image de l'Espagne à l'étranger, la diffusion de photographies violentes ne correspondant pas à l'événement en question en est un exemple clair (Palmer, 2017).

À cette occasion, on comprend mieux la phrase prononcée par Hill (2021) : « *the fire was already burning ; all Putin had to do was pour on some gasoline* ». Donc une certaine « auto-mutilation » de sa propre démocratie s'était déjà produite, en plus d'être alimentée par ce flot *fake news* sur le web.

b) Discréditer les institutions européennes et l'ordre socio-libéral (représenté par les États-Unis).

Étant donné que l'UE défend des valeurs libérales et prône la résolution pacifique des conflits, il n'est pas surprenant que la crise catalane constitue un défi pour l'UE (Emmott, 2017). Le simple fait de convoquer une consultation citoyenne illégale et anticonstitutionnelle au sein d'un État membre représente une attaque intrinsèque contre l'État de droit et la démocratie, deux valeurs parmi les plus fondamentales de l'UE. En plus, le ton violent de la tentative d'empêcher la tenue du référendum peut aussi facilement être considéré comme une « auto-attaque » contre ses propres fondements ; et ergo comme une victoire pour la Russie. C'est pourquoi, toute diffusion par rapport au 1-O serait favorable à la Russie, étant donné son identité anti-occidentale et ses aspirations néo-réalistes.

Au niveau social, si on regarde quelques statistiques pour voir le taux de préoccupation parmi la citoyenneté européenne ; on remarque que, par exemple, 48% (des Italiens) considèrent que la crise catalane concerne l'UE dans son ensemble, malgré son apparence de *question interne* (Statista Research Department, 2020). En fin de compte, l'UE est perçue comme la garante de la paix et de la stabilité européennes. D'ailleurs, après le référendum, une déclaration unilatérale d'indépendance du gouvernement catalan a eu lieu (Serra et al., 2018), ce qui n'est pas une petite affaire et soulève directement l'une des questions parmi les plus sensibles : la souveraineté nationale. Il est impossible de démontrer dans quelle mesure la cyberactivité russe a pu influencer le sentiment de malaise des citoyens européens, mais elle a certainement tiré la sonnette d'alarme.

De plus, après une première impression malheureuse de la gestion de la crise par l'État espagnol le 1-O, l'opinion publique européenne s'est progressivement orientée vers une position plus critique vis-à-vis de l'indépendance (Benito, 2017). En effet, le propre vice-président de la Commission européenne de l'époque, M. Timmermans, a déclaré que « la Commission Européenne n'a aucune critique à formuler sur le fonctionnement de la démocratie espagnole, la séparation des pouvoirs et l'application des droits de l'homme ». Et peu après, le Rapport Annuel sur la Citoyenneté de l'UE a été adopté, autorisant la condamnation des gouvernements régionaux s'ils enfreignent une loi ou modifient les frontières, portant ainsi préjudice à l'exercice de la citoyenneté européenne (en Molina & Martín, 2019). C'est-à-dire, l'état de l'UE a même été renforcée.

En résumé, l'initial sentiment de sympathie inspiré en Europe par la Catalogne, produit d'une perception en tant que « parti faible » -ce à quoi l'activité russe a contribué- ; a été rapidement remplacé par un soutien à Madrid (Molina & Martín, 2019). Et le résultat final n'a pas été aussi fragmenté comme elle l'avait prévu. Du fait, l'image extérieure de l'Espagne se trouvait dans le poste numéro 14 de prestige mondial et le numéro 3 au niveau européen juste deux années après le 1-O (Molina & Martín, 2019). Cela indique que, malgré les dommages initiaux, l'objectif d'affaiblissement visé n'a pas été atteint à court terme. Toutefois, on s'interroge si au plus long terme, la cyber-attaque russe pourrait jouer un rôle important dans le cadre du processus sécessionniste.

3.4.2. Polarisation de la population

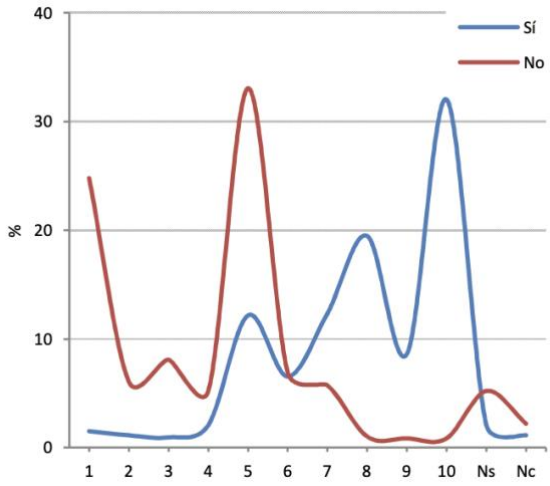
Comme Al Jazeera (2017) l'a décrit : « les médias reflètent la tension de la rue », bien que l'élément social soit parfois négligé. Dans ce cas en revanche, il est essentiel de connaître l'impact social des événements, en spécial quand les médias ne favorisent pas le rapprochement. La grande tension politique qui est apparue entre les citoyens -particulièrement pendant les jours précédant le 1-O et le 1-O lui-même- a été très forte ; pas justement entre les catalans mais aussi entre les catalans et le reste d'espagnoles. En plus, on a vu des manifestations spectaculaires ainsi qu'une grève générale après les événements du 1-O (France 24, 2017) ; qui corroborent le sentiment de malaise social.

En effet, l'auteur russe Georgii Pocheptsov (2017) a mis en lumière l'importance de l'information et comment sa manipulation peut conduire à un vrai changement de comportement dans les personnes. Dans ce sens, il est intéressant de citer l'analyse de la politologue Berta Barbet, qui a défini l'impact social vécu en 2017 en Catalogne avec deux mots : « déconnexion » et « rupture ». « Déconnexion » parce que les catalans ont arrêté d'écouter les arguments de la partie adverse ; et « rupture » car la colère accumulée a influencé sur les relations personnelles dont certaines ont pris fin en raison de désaccords politiques. Du fait, 40% des catalans avaient stoppé de parler politique avec ses amis et famille. Cette dissociation entraîne une détérioration grave de la coexistence et implique une réduction des valeurs communs en communauté (Ordaz, 2017).

Si nous transposons ce phénomène au monde en ligne, nous constatons que les réactions des utilisateurs aux messages pro-indépendance ont été beaucoup plus positives que celles des messages non-indépendance. Ceci est encore plus accentué dans le cas des informations diffusées par RT et notamment lors de la diffusion des protestations citoyennes suite à l'arrestation du président de la communauté autonome de l'époque (López-Olano & Fenoll, 2020). Cela signifie que l'indépendance et le soutien en sa faveur ont atteint leur apogée dans les jours autour du 1-O, exactement au moment où la cyberactivité de la Russie était la plus forte (Krah, 2021). De plus, comme on verra dans le graphique suivant, le soutien populaire à l'indépendance catalane chute après le mois d'octobre en 2017 et ergo après l'incident du 1-O (Medina, 2018) ; coïncidant avec la réduction de l'activité provenant de sources russes (Krah, 2021).

Figure nº 3 : Sondage d'opinion en Catalogne en 2017 sur leur soutien à l'indépendance.

La question à laquelle ce graphique suivant répond est : « *Voulez-vous que la Catalogne soit un État indépendant ? »*



(Medina, 2018, p. 4)

Ceci dans une certaine mesure, nous permet d'établir des relations entre la polarisation sociale et le soutien à l'indépendance catalane vis-à-vis les cyber-attaques russes. Toutefois, l'ingérence russe n'a pas été l'unique source de polarisation et d'agitation de la population. En réalité, ce résultat est aussi dû à d'autres facteurs comme la désescalade de la tension due au passage du temps ou la relaxation des médias nationaux par rapport à la couverture des événements. Ce dernier point est dû au fait que les moments de tension politique particulière permettent aux media de se positionner et d'afficher un discours clair d'attribution de la culpabilité, en recourant souvent à des valeurs et des arguments typiques d'un climat de polarisation (Teruel, 2013).

En résumé, les actions telles que celles mentionnées ci-dessus ont eu un impact, notamment au niveau de la citoyenneté. D'un part, la divulgation de contenus en support de la cause indépendantiste par le biais de moyens tels que Twitter avant et pendant le Référendum du 1-O 2017, a favorisé le soutien de l'opinion publique. Néanmoins, on ne peut pas démontrer une relation plus forte entre l'élection massive pour l'indépendance (Le Soir, 2017) et la possible désinformation d'origine russe dont ils auraient fait l'objet. D'autre côté, la diminution de la cyberactivité en provenance de la Russie après le 1-O pourrait avoir eu un rapport avec la réduction du soutien des citoyens à la cause indépendantiste, parmi des autres facteurs comme le passage du temps ou le relâchement des médias nationaux.

4. LES ÉLÉCTIONS FRANÇAISES EN 2017

4.1. Présentation de faiblesses-cible en France

Aussi ancienne que soit cette Nation, leur nature pessimiste et leur déception envers la classe politique est quelque chose qui reste dans le temps. En effet, un des éléments les plus caractéristiques du paysage politique en France est la vision négative étiquetée à la classe politique française. Ce fait a été souligné par plusieurs statistiques comme le « Political Trust Barometer » ou le « Global Trustworthiness Index ».

En effet, le niveau de méfiance sociale envers les institutions de l'État et leur capacité à résoudre les problèmes, est comparativement plus faible que dans d'autres pays d'Europe. Quand les citoyens ont été interrogés pour l'enquête, 41% ont ouvertement exprimé un sentiment de « lassitude » par rapport à leur état d'esprit en matière de politique, suivi par « abattement » (34%) et « méfiance » (28%). Si l'on compare avec d'autres pays comme l'Allemagne ou le Royaume-Uni, on constate une grande différence, puisque dans ces pays, la première réponse des citoyens était la « sérénité » (Cautrès, Ivaldi & Rouban, 2021).

En somme, les sentiments de désillusion et de désenchantement à l'égard de la classe politique et du fonctionnement de l'État français permettent de l'utiliser comme cible pour galvaniser des citoyens vers l'extrême droite et le populisme. Cela étant dit, au moments clés ou de tension, les citoyens croiront aussi loin qu'ils « veulent croire », ce qui n'est pas nécessairement la vérité. C'est à ce moment que la désinformation et les *fake news* peuvent agir comme un véritable catalyseur de la polarisation. Ainsi, cette lassitude à l'égard de la classe politique française fait qu'il est facile pour un scandale, aussi minime soit-il, à la veille des élections, d'avoir un effet fatal sur le résultat électoral du candidat.

Cela signifie que, comme nous l'avons expliqué plus haut, les faiblesses internes d'un État, comme dans ce cas le mécontentement généralisé des citoyens, peuvent être encore plus polarisées ou attisées dans les moments de tension à travers la cyber-attaque. Nous rappelons que selon Larousse, un moment de *tension* peut être une « situation tendue entre deux groupes ou deux personnes » ; et il n'y a pas de meilleur exemple pour illustrer cela

qu'une élection, qui se caractérise par l'opposition d'idées, représentées par les différents candidats.

Ayant dit ça, il convient de noter que le cas en question est important parce qu'il a été un échec à court terme : le résultat de l'élection n'a pas coïncidé avec l'objectif des (cyber)attaquants, qui était d'empêcher l'accession au pouvoir de Macron (Jeangène, 2019). Toutefois, on doit se demander quel impact à plus long terme cela pourrait avoir sur la montée de l'extrême droite.

4.2. Raisons de la Russie

La propagation d'origine russe des certaines informations a eu pour but d'alimenter le débat public, prenant clairement la position de la droite française en soutenant des candidats comme Marine Le Pen ou François Fillon (Pétiniaud & Limonier, 2018).

Si on se demande pourquoi, dans ce cas, la cible est les personnalités et non les partis politiques ; la réponse est simple : la menace la plus importante au niveau de cyber-attaques en France -particulièrement pendant des élections- est le dommage causé à la réputation des candidats. Le vol des informations personnelles ou de mots de passe et sa diffusion conséquente, peut avoir un effet multiplicateur en termes d'opinion publique et donc d'intentions de vote (Tauziac, 2017). Surtout pour les plus indécis, dont le vote peut facilement être influencé par un scandale de dernière minute.
Dans cette optique, il est intéressant de noter les déclarations Julien Nocetti, chercheur à l'Institut français des relations internationales. Il a déjà fait savoir à l'époque que « *en 2017, il y a une sorte d'alignement des planètes pour le Kremlin avec trois candidats prorusses : François Fillon, Marine Le Pen et Jean-Luc Mélenchon. Or Macron n'est pas du tout sur cette ligne* » (en Tauziac 2017, pár. 11). Il n'est donc pas surprenant que Marine le Pen ait été vue serrant la main de Poutine à la veille du premier tour des élections de 2017[13] ou ait fait des remarques flatteuses ou admiratives à l'égard du président de la Fédération Russe au fil des ans (Geoffroy & Vaudano, 2022).

[13] Même si actuellement, Marine le Pen nie tout lien entre elle et son parti à Poutine, vu l'invasion russe de l'Ukraine (Geoffroy & Vaudano, 2022).

Après tout, la Russie, dans sa logique réaliste, cherche à faire valoir ses intérêts sur la scène internationale (Joseph, 2014), et quel meilleur moyen de le faire que d'avoir pour allié l'un des États membres de l'UE les plus influents? Le vote quasi systématique des eurodéputés du Rassemblement National au Parlement Européen contre les résolutions condamnant la Russie -jusqu'à son invasion de l'Ukraine en 2022- (Geoffroy & Vaudano, 2022), ou la position de M. Fillon, toujours en faveur de la levée des sanctions imposées à la Russie à la suite de l'annexion de la Crimée (Vitkine, 2016) ; expliquent pourquoi ces deux candidats soient laissés à l'écart des cyber-attaques.

En somme, si le Rassemblement National (en 2017 appelé Front National) ou Les Républicans avaient remporté les élections en 2017, ça aurait eu sans doute des effets bénéfiques pour la Russie. À titre d'exemple, le parti de Le Pen, étant anti-européen (Rassemblement National, 2017) aurait pu déclencher un *Frexit* s'il avait remporté les élections ; et ainsi aurait porté un coup dur pour l'UE et ses valeurs libérales. Également, la Russie aurait été ainsi plus proche de « se faire respecter » et de retourner à la « table de négociations » au niveau international (Pavlova & Romanova, 2012) ; d'un point de vue théorique, une manifestation du néo-réalisme, dans le sens où les pressions dites systématiques affectent la politique étrangère russe (Firoozabadi & Ashkezari, 2016).

4.3. Événements

Tout d'abord, on va préciser que les élections françaises en 2017 ont eu lieu le 23 avril et le 7 mai, respectivement les dates du premier et du deuxième tour. Au premier tour, Macron a obtenu 24,01% des voix et Marine le Pen le 21,30%. Au deuxième tour, l'avance de la République En Marche sur le Front National a été encore plus grande, le parti de Macron 66,10% et celui de Le Pen 33,90% (Ministère de l'Intérieur, 2017).

Sur cette base, on va établir les événements proches aux élections liées à la Russie soit par moyen des médias, soit à travers les réseaux sociaux ; afin de pouvoir établir l'impact possible causé par cette cyberactivité. Pour ça, nous nous concentrerons sur la fluctuation en intention de vote des Français, même si le résultat final des élections n'a pas été celui escompté par les cyberattaquants.

Au niveau technique, la campagne de sabotage de Macron a été caractérisée par le fait qu'elle a respecté un processus classique d'opérations d'information, ainsi dénommé « *Hack And Leak* ». De cette façon, le cycle suivi par l'information a été le suivant :

a) Obtention d'information secrète par piratage ;
b) Construction d'une narrative par rapport à ces informations (éventuellement mélangées avec des informations fausses et de leurre) ; et
c) Diffusion d'une partie aux médias sociaux et à la presse, provoquant ainsi une désinformation. Un exemple bien connu qui a suivi cette logique est celle du « MacronLeaks » (Jeangène, 2019).

À cet égard, il faut clarifier que, même si l'audience de RT et Sputnik en France n'est pas très élevée, leurs contenus ont été largement disséminés en suivant le processus susmentionné. L'image (cfr. Annexe I), illustre cette procédure de manière plus graphique afin de mieux le comprendre.

4.3.1. Premier tour: 23 avril 2017

Les rumeurs et insinuations défavorables à Macron et visant à déplacer les intentions de vote vers d'autres candidats tels que Marine le Pen, se sont accentués au cours des mois de janvier et février, au même moment où la popularité de Macron a commencé à menacer les autres candidats. À ce propos, on doit spécifier que la chute de popularité du candidat Fillon en raison du scandale impliquant son épouse a clairement aidé à la hausse de la popularité de Macron (Jeangène, 2019). Ces faits se sont surtout déroulés à travers les médias -russes et occidentaux- et Twitter, comme on verra dans les sous-sections suivantes.

- Les médias russes : RT et Sputnik

Par rapport aux médias qui ont été impliqués dans ces actions, nous devrions ajouter que la plupart des contenus provenant de la Russie ont été dévoilés par la holding publique russe Rossija Segodnja, propriétaire de Sputnik et RT (Pétiniaud & Limonier, 2018). Toutefois, certains médias occidentaux (surtout ce que l'on appelle *l'alt-right américaine*) ont également encouragé certaines attaques contre Macron (Jeangène, 2019), mais nous ne nous étendrons pas sur ce sujet dans ce travail.

Des nombreux articles de presse et interviews ont été publiés par les médias russes Sputnik et RT concernant Macron. Un exemple a été l'article de presse publié le 3 février par un journal russe, intitulé « *Assange va jeter de l'huile sur le feu de la campagne présidentielle en France* », où le fondateur de *WikiLeaks* assurait avoir des informations relatives à Macron obtenues grâce au piratage d'Hillary Clinton. Ensuite, Sputnik a publié un autre article en dépeignant Macron comme un « *agent américain soutenu par un très riche lobby gay* ». Ces déclarations conduiront à Macron lui-même à s'excuser, allant même jusqu'à nier une relation homosexuelle extraconjugale, alors qu'aucun argument ne vient étayer cette accusation (Jeangène 2019, p. 4).

En outre, le 9 février, Sputnik a republié en affirmant qu'il y avait des journalistes français à Moscou en portant des t-shirts de propagande de La République En Marche. En faisant cela, ils voulaient faire croire que les médias plus traditionnels eux-mêmes étaient biaisés en faveur de Macron. Heureusement, cela s'est avéré faux. Il est intéressant de noter que Margarita Symonian, l'éditrice principale de Sputnik et RT, s'est défendu en disant que ces informations provenaient de citations, et alors de sources fiables, même si l'information était fausse (Jeangène, 2019).

Dans ces conditions, il est difficile d'affirmer catégoriquement que ces médias ont inventé du contenu, mais plutôt qu'ils ont manipulé les informations à leur disposition : étant biaisés, omettant des informations importantes et mettant en évidence ou supprimant certaines citations. Il leur est ainsi plus facile de créer une « illusion de vérité », qui n'est pas réelle (Jeangène, 2019).

- Twitter

Twitter a joué un rôle plus important avant le second tour des élections qu'au premier tour, d'où la brièveté de cette sous-section. Toutefois, nous donnerons un exemple.

Le 2 mars a commencé une autre campagne de désinformation qui a mis en doute le financement du parti de Macron et l'a lié avec l'Arabie Saoudite. Étonnamment, le lien URL a été cloné du journal Le Soir, ce qui donne l'impression qu'elle provient réellement de la source belge. En dépit de l'absence d'auteur, les bénéficiaires

potentiels et la capacité à les porter ne permettent pas à la Russie de s'en tirer à bon compte. En plus, Marion Maréchal-Le-Pen, députée et nièce de Marine le Pen, a ensuite partagé sur son compte Twitter en titre accusateur qui a reçu plus des 200 retweets dans une demi-heure (Jeangène, 2019).

4.3.2. Deuxième tour: 7 mai 2017

Étant donné que la plupart des activités perturbatrices émanant de la Russie au cours du second tour ont été menées via les réseaux sociaux, nous nous concentrerons sur ces derniers dans cette section.

- Presse : Sputnik et RT

Au second tour des élections, la cyberactivité la plus importante a été liée au « MacronLeaks ». C'est pourquoi la fonction perturbatrice des médias russes RT et Sputnik s'est déplacée vers le monde de réseaux sociaux. À cet égard, les comptes Twitter de ces journaux ont retweeté les messages qu'on expliquera davantage ci-dessous et ainsi ont favorisé la diffusion des *fake news*.

- Twitter

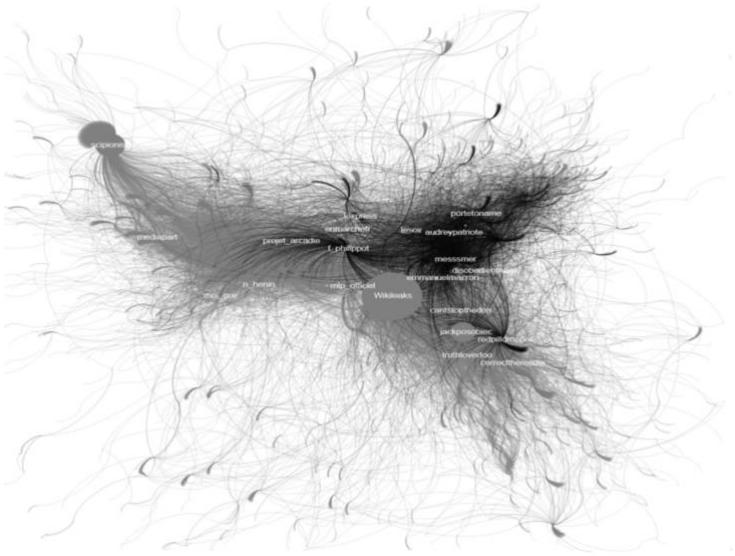
L'exemple le plus connu de cyberactivité troublant au deuxième tour a été celui du « *Macronleaks* », puisque sa couverture médiatique a été considérable. Toutefois, il faut préciser que le #MacronLeaks avait été créé en 2016 avant les élections américaines, pour ressurgir avec force à la veille des élections présidentielles françaises (Jeangène, 2019). À cette occasion, la source de la controverse se situe le 3 mai 2017, lorsqu'une adresse IP lettonne a posté deux faux documents sur le réseau anonyme 4chan qui suggèrent que Macron avait un compte bancaire secret dans l'une des îles Caïmans (Jeangène, 2019). Curieusement, l'accusation concernant le compte bancaire qui venait d'être dévoilée, a été évoquée par Marine Le Pen dans les dernières minutes du débat électoral le 3 mai même (Pétiniaud & Limonier, 2018).

Puis, le 5 mai, le tweet catalyseur étiqueté comme #MacronLeaks a été publié en Twitter et en s'associant aux articles d'Assange. En plus, dans les trois heures, environ 47.000 autres comptes ont utilisé le même hashtag en remplissant Twitter et étant accompagné par d'autres hashtags similaires comme #MacronCacheCash (Hernández, 2020). Cela suggère clairement l'intervention susmentionnée de *bots* et de *trolls*, étant un élément important d'amplification de la dissémination. De cette façon, une diversité de fausses informations a inondé les réseaux sociaux le jour même de la fin de la campagne électorale. Parmi les *fake news* le plus frappantes figuraient l'existence d'un compte bancaire caché dans un paradis fiscal appartenant à Macron, l'achat des drogues par l'équipe de la République En Marche à des députés français et le trucage des élections (Jeangène, 2019).

En outre, les « *Macronleaks* » doit être compris comme un ensemble contenant environ 150.000 fichiers. Ces documents avaient été obtenus sur l'équipe de Macron à travers des opérations successives de *phishing* (Pétiniaud & Limonier, 2018), dont l'auteur avait été lié à des groupes de piratage russes tels que *Fancy Bear* ou *Pawn Storm* (Hernández, 2020). Des attaques successives de vol d'informations avaient déjà été signalées par l'équipe de campagne de Macron à plusieurs reprises (Jeangène, 2019).

Pour en revenir à la question de la diffusion de masse des « MacronLeaks », la viralité à laquelle ces informations ont donné lieu n'est pas été justifié par la nature du contenu, pointant l'intervention probable de *trolls* et de *bots*. De plus, l'inondation des réseaux sociaux avec des *fake news* à travers l'utilisation de hashtags, rend cet enjeu plus complexe. C'est pourquoi, afin de faciliter la compréhension, on va expliquer la relation entre l'arborescence « Macronleaks » et les comptes Twitter « pro-russes » à travers une image qui montre son interrelation (Petiniaud & Limonier, 2018).

Figure nº 4 : Interaction entre « Macronleaks » et les comptes Twitter « pro-russes ».



Données Twitter récoltées par les auteurs *via* NodeXL.

(Pétiniaud, & Limonier 2018, p. 324)

Cette image regroupe tous les comptes actifs pendant la campagne des « Macronleaks » - étant celui du Wikileaks au milieu en raison de sa mention par d'autres comptes-, et les divise en trois :

a) Les comptes anglophones qui ont fait grand usage du mot-clé « Macronleaks » et procédant de sources pro-Trump sont situés en bas à droite.
b) Les comptes francophones défavorables à Macron et partisans des documents piratés se situent en haut à droite.
c) Des comptes contraires à l'extrême droite se trouvent en haut à gauche.

Quand nous regardons cette image, nous devons savoir que l'intensité du couleur et la quantité des lignes représentent non seulement le nombre des comptes en Twitter associés avec certaines idées, mais aussi les interactions avec ceux-ci (Pétiniaud & Limonier, 2018). Également, les figures noires sont classées comme provenant de plateformes russes et sont celles en faveur de l'extrême droit française. Ce qui est le plus surprenant, c'est l'hyperactivité de ces comptes -par rapport aux autres deux groupes-, et malgré le faible nombre de comptes confirmés comme étant le soutien d'actions informatives russes. Du fait, les comptes pro-russes ont posté deux fois plus de tweets que les autres, atteignant même le chiffre de 28 tweets par heure. Ainsi, la

viralité du mot-clé a connu un grand succès et a insinué une programmation automatique évidente (Pétiniaud & Limonier, 2018).

La figure (cfr. Annexe III) démontre aussi que la twittosphère russe est clairement orientée vers l'extrême droite, c'est-à-dire plus proche de l'idéologie promue par Le Pen (Pétiniaud & Limonier, 2018).

4.4. Impact en France

Pour analyser l'impact possible que les cyber-attaques ont eu pendant la campagne électorale en 2017, nous nous concentrerons sur les sondages d'intention de vote. À cet égard, au cours de ce chapitre nous fournirons des graphiques -dans le texte et dans l'annexe- pour appuyer nos déductions. De cette forme, nous essayerons de mettre en relation les périodes de majeure désinformation et cyber-activité en provenance de la Russie, et le changement en intention de vote des citoyens français.

Cependant, nous devons savoir dès le départ que même si la cyberactivité russe a pu encourager certaines fluctuations dans les intentions de vote -en plus d'autres facteurs- l'objectif à court terme a été un échec puisque Macron a remporté l'élection. Cela signifie que malgré la désinformation et les *fake news*, l'opinion publique française ne s'est pas livrée à une manipulation pure et simple au moment du vote.

4.4.1. Premier tour: 23 avril 2017

Le sondage Ipsos-Sopra Steria (cfr. Annexe IV) qui a été réalisé les 12 et 13 avril 2017 démontre la proximité entre tous les candidats en tête, mais surtout entre Macron (22%) et le Pen (22%). En plus, il souligne que par rapport au pourcentage de 85% des répondants qui affirmaient que leur vote pour Le Pen était définitif, seul 68% de ceux qui se déclaraient électeurs de Macron garantissaient leur vote pour La République En Marche. En définitif, l'égalité entre Le Pen et Macron à l'approche du premier tour était impressionnante (Courtois, 2017).

Nous analyserons ci-dessous un graphique montrant la fluctuation des intentions de vote envers les candidats les plus populaires dans les mois précédant le premier tour.

Figure nº 5 : Sondage sur les intentions de vote dans les jours précédant au premier tour effectué par Financial Times.

Wisniewska, A., Locke, C., Nevitt, C., & Rininsland, A. (2017, 7 May). French presidential poll tracker 2017. *The Financial Times*. Last Retrieved on the 16th of May 2022 from https://ig.ft.com/sites/france-election/polls/

Si on observe ce graphique attentivement et on le met en relation avec les événements précédemment décrits, on sera mieux à même de spéculer sur les effets possibles de l'ingérence russe. Cependant, il faudra être conscients du fait que cette fluctuation est évidemment affectée par d'autres facteurs excluant la cyberactivité russe.

Premièrement, on sait qu'en janvier et février 2017 les rumeurs et insinuations contre Macron s'intensifiaient (Jeangène, 2019), à un moment où la popularité de Macron semblait prête à décoller. Et deuxièmement, cela coïncidait avec le moment où Fillon perd en popularité à cause de « *l'Affaire Fillon*[14] » (ou « *Penelopegate* ») en permettant ainsi que Macron se positionne presque en tête des sondages. Ces faits indiquent que la

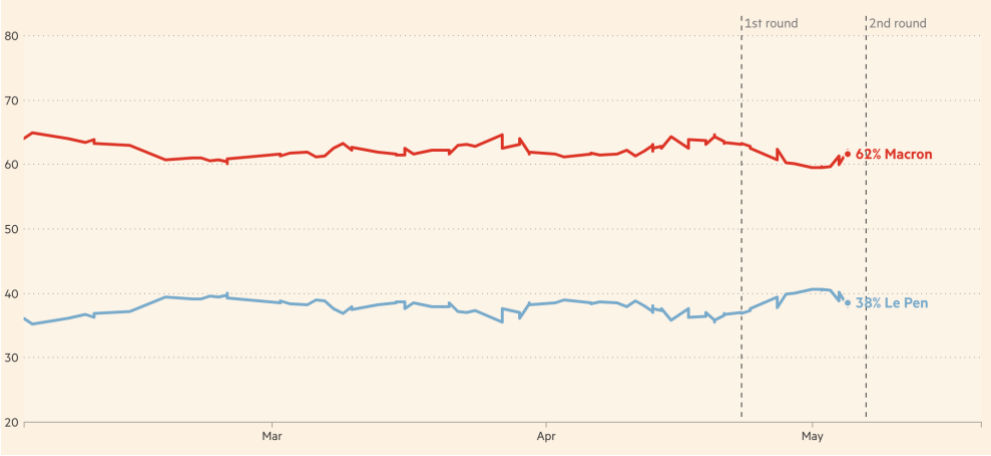
[14] Scandale de corruption impliquant son épouse Penelope Fillon, qui a éclaté au grand jour pendant la campagne électorale de 2017. Ainsi, bien que faisant partie des favoris dans les sondages, il a été éliminé dès le premier tour (Mazuir, 2021).

désinformation croissante vis-à-vis Macron au cours de ces mois n'était pas une coïncidence, mais qu'elle visait plutôt à atténuer le « *blowback* » d'autres candidats tels que Fillon. En même temps celle-ci nuisait à la réputation de Macron. Autrement dit, il est possible que la popularité de Macron aurait pu augmenter plus rapidement, s'il n'y avait pas eu des cyber-attaques russes menaçant les sondages de vote.

Néanmoins, on ne peut pas tomber dans le réductionnisme et limiter la scène politique/électorale d'un État aux seuls effets de la cyberactivité russe. En fin de compte, il y avait d'autres facteurs d'influence, tels que la performance des candidats pendant la campagne électorale ou le changement d'avis des électeurs eux-mêmes. Quoi qu'il en soit, l'histoire a montré que Macron a surpassé Le Pen et les autres candidats au premier tour, donc l'objectif principal d'empêcher Macron de gagner n'a pas été atteint.

4.4.2. Deuxième tour: 7 mai 2017

Figure nº 6 : Sondage sur les intentions de vote dans les jours précédant au deuxième tour effectué par le Financial Times.



Wisniewska, A., Locke, C., Nevitt, C., & Rininsland, A. (2017, 7 May). French presidential poll tracker 2017. *The Financial Times*. Last Retrieved on the 16th of May 2022 from https://ig.ft.com/sites/france-election/polls/

Comme nous l'avons déjà mentionné, l'interférence russe au second tour s'est caractérisée par la diffusion massive de (dés)information sur les réseaux sociaux, l'insistance de celle-ci contre Emmanuel Macron étant remarquable. En ce sens, les manœuvres effectuées en ligne par la Russie pour diffuser des informations telles que les « #Macronleaks » représentent un soutien symbolique à Marine Le Pen.

De plus, cet obscurcissement contre le candidat de la République En Marche c'est accentué à 4 jours du second tour, en raison de la force des « #MacronLeaks » ; qui aurait pu avoir un impact sur les intentions de vote début mai. Si l'on prête attention au graphique, on constate une hausse éphémère de la popularité de Le Pen, alors qu'en même temps, on observe une baisse de celle de Macron. Même si d'autres facteurs avaient influencé la situation, il semble raisonnable de penser que cette fluctuation minime pourrait être due au scandale des « #MacronLeaks ».

En fin de compte, Macron a remporté l'élection, donc l'influence russe n'a pas eu l'effet escompté à court terme, ce qui n'exclut pas qu'à long terme, elle puisse avoir un effet sur la croissance de l'extrême droite (Kamiya, Kang, Kim, Milidonis & Stulz, 2018). Il n'en reste pas moins qu'il s'agit d'une attaque majeure contre la démocratie d'un État et d'un nouvel exemple de l'appétit d'influence néo-réaliste dans la sphère internationale.

5. BRÈVE COMPARAISON ENTRE LES DEUX CAS

L'analyse des deux cas présentés dans ce travail, démontre la mise en œuvre de la soi-disant « Nouvelle Doctrine Militaire » par la Fédération Russe en 2014, qui vise à exercer de l'influence à l'étranger, spécifiquement à travers le cyberespace. À cette fin, l'hétérogène « russosphère » et les médias russes, ont été mis au service des objectifs de cette cyber-stratégie (Pétiniaud & Limonier, 2018), comme on a vu tout au long de ce travail. Ci-dessous, nous ferons une comparaison à travers les objectifs, la façon dont ils ont été réalisés et le succès obtenu.

5.1. Objectifs-raisons

En ce qui concerne les objectifs de la Russie en s'engageant dans un tel comportement, le fait que les deux États fassent partie de l'UE, a constitué une raison majeure du

ciblage. Cela est dû à la position de l'UE en tant que garante de la démocratie libérale et des valeurs occidentales. C'est pourquoi, un mouvement sécessionniste réussi en Europe ou l'accession au pouvoir de la droite radicale eurosceptique dans un pays comme la France, aurait déclenché des sonnettes d'alarme au sein de l'UE. Une projection de la démocratie libérale comme défaillante ou une poussée du sentiment anti-occidental et son modèle (Milosevich, 2017 b), se seraient avérés comme une victoire -même symbolique- pour la Fédération Russe.

Si nous ramenons cela à l'étude de cas particulière, les objectifs à grande échelle du Kremlin -déjà évoqués-, auraient pu être aidés par son cyberactivité dans ces deux États. Par rappel, en Espagne, ils tentaient de porter atteinte à sa démocratie et d'attiser la polarisation sociale ; alors qu'en France, ils visaient à détériorer l'image du candidat de la République En Marche, au profit d'autres comme Le Pen. En tout état de cause, les faiblesses structurelles de chaque pays, ont été profitées par les cyber-attaques dans les moments de grande tension pour endommager les valeurs occidentales (Milosevich, 2017 b). En d'autres mots, les intérêts de la Russie seraient servis au-delà de ses frontières en tant qu'adeptes du réalisme néoclassique (Firoozabadi & Ashkezari, 2016) et exalteraient la position de la Fédération Russe dans le système international (Alandete, 2017 a)

5.2. Modus operandi

Par rapport à la manière de perpétrer les cyber-attaques, l'usage de la « viralité du mot-clé » a été essentiel dans la stratégie disruptive en favorisant l'association d'un évènement particulier avec un mot. Par exemple, dans le cas français le mot « Macronleaks » a reçu une grande interaction sur Twitter, comme en Espagne le mot « dictature ». Cela est dû à l'hyperactivité des comptes pro-russes dans des réseaux sociaux comme Twitter, en provoquant une diffusion démesurée portée par l'utilisation de *bots* et *trolls* (Pétiniaud & Limonier 2018, p. 325).

Toutefois, la (des)information promue par le Kremlin dans ces deux États, ne s'est pas déroulée de la même manière. D'une part, en Espagne, l'utilisation de « partenaires » tels qu'Assange a eu un rôle fondamental pour diffuser des informations totalement fausses et intolérantes afin de diviser l'opinion publique. D'autre part, en France, les

informations disséminées, ont été obtenues par des campagnes de *phishing* successives, qui d'ailleurs étaient plutôt déformées et biaisées (Jeangène, 2019). Ainsi, le processus employé pour diffuser l'information a été le même (cfr. Annexe II.)

En outre, on observe une tendance où les cyber-attaques sont utilisées pour booster un contexte de confrontation dans les moments de tension. Cela se fait par l'opposition de deux notions contraires comme être en faveur ou contre l'indépendance en Espagne ou être en faveur ou contre la « droite radicale » en France. Dans le premier cas, la célébration d'un référendum inconstitutionnel -événement extraordinaire- a servi de moyen pour la mobilisation sociale et, en conséquence, de cible pour un éventuel « réchauffement social ». Dans le deuxième cas, la mauvaise presse pour l'un des candidats, pourrait provoquer un mécontentement public encore plus grand envers l'environnement politique, poussant l'électeur vers des options plus radicales. Selon Pocheptsov (2017), il arrive parfois qu'un choc dans la « vie physique » résulte d'un « réchauffement » précédant stimulé par la « vie en ligne ».

5.3. Succès

Partant du constat que les objectifs envisagés à court terme par la Russie dans chacun des États n'ont pas été atteints. La démocratie espagnole est toujours perçue de manière positive et le climat de tension dans la société espagnole et le soutien à l'indépendance c'est amoindrie ; et bien que Macron ait gagné les élections, nous dirons ce qui suit.

Tout en tenant en compte la corrélation entre l'augmentation de la cyberactivité de la Russie et les effets nuisibles sur l'Espagne -y compris une plus grande polarisation citoyenne et les dommages initiaux à la réputation espagnole-, cela suggère que ceux-ci pourraient avoir un impact sur la scène politique. Cependant, il faut être conscients que le déroulement des événements est influencé par de nombreux facteurs et qu'il est difficile à démontrer ce lien cyber-attaque - impact.

Malgré les tentatives de dégradation de son image avant l'élection, il a remporté les deux tours. Cela indique déjà un échec plus important de l'intervention russe en comparaison avec les attaques destinées vers l'Espagne. Quant à la relation entre les fluctuations des intentions de vote au détriment de Macron et une plus grande diffusion de l'information

biaisée, elle pourrait exister, comme nous l'avons montré mais amoindrie. Également, il est difficile de le prouver étant donné l'existence d'autres facteurs d'influence externes tels que *l'Affaire Fillon* ou la performance dans le débat électoral (Pietralunga, Bonnefous et Faye, 2017). À cet égard, les Français, semblent avoir été moins perméables à certaines revendications dont la véracité était douteuse.

Tout ceci suggère que le plus qu'une société soit polarisée, le plus est-t-elle susceptible de succomber aux effets d'une cyber-attaque, bien que ce climat de tension était beaucoup plus élevé en Espagne par rapport en France, vu la longue histoire du processus sécessionniste catalan.

6. CONCLUSION

Durant tout ce travail, nous avons souligné l'importance du cyberespace comme outil de la politique étrangère russe. De fait, nous avons essayé de démontrer certains liens entre des cyber-attaques telles que la diffusion de *fake news* sur Twitter, ainsi qu'un léger effet disruptif dans la scène politique d'un pays à travers une étude de cas. De plus, nous sommes arrivés à la conclusion que ces interférences ne sont pas le fruit du hasard, mais surviennent durant des moments de grande tension au sein de l'État et exploitent les faiblesses structurelles. Toutefois, il faut être conscient de la difficulté de tester la corrélation entre ces deux variables et savoir que lorsqu'on analyse ce type de phénomènes, nous nous basons notamment sur des spéculations (Kamiya et al., 2022).

Similairement, nous pouvons ajouter que l'intervention étrangère dans les élections ou les consultations citoyennes n'est pas nouvelle. En effet, tout au long de l'histoire, de nombreuses puissances ont tenté d'influencer le résultat des élections dans un État ; soit pour aider ou gêner un candidat, soit pour nuire au processus démocratique de l'État en question. Cela met à nu la logique réaliste -maintenant réadapté par la Russie en forme de réalisme néoclassique- qui pendant tant d'années a été exclusivement suivie dans les relations internationales (Joseph, 2014). Cependant, au cours des dernières décennies, les progrès de l'Internet et des réseaux sociaux ont facilité la croissance d'informations manipulées sur le web (Fonfría & Duch-Brown, 2020). En effet, certaines circonstances déjà existantes dans la société, telles que la désillusion des citoyens vis-à-vis de la classe

politique ou la polarisation identitaire, expliquent en partie le ciblage de certaines personnes de ces cyber-attaques (Jeangène, 2019).

Par rapport aux cas concrets analysés, en Espagne, on observe une corrélation entre l'augmentation de la cyberactivité de la Russie pendant les jours précédents ainsi que ceux consécutifs au 1-O, et certains effets disruptifs dans sa scène politique, telle qu'une mauvaise presse initiale de la réputation de l'État ainsi qu'une croissance de la polarisation sociale. Cependant, prouver la causalité entre les deux variables est presque impossible. Par conséquent, on se retrouve avec des spéculations dont la relation reste raisonnable compte tenu des données. Concernant la France, on est dans une situation similaire dans le sens où la fluctuation des intentions de vote et la cyberactivité pourrait être liées. Cependant, il est très difficile de le prouver au vu de l'influence d'autres facteurs comme *l'Affaire Fillon* ou de la performance dans le débat électoral dans la scène politique (Pietralunga, Bonnefous et Faye, 2017).

Quoi qu'il en soit, nous pouvons conclure brièvement, qu'à court terme, les cyber-attaques russes en Espagne et en France ont échoué. D'un part, la réputation démocratique de l'Espagne reste positive et les tensions sociales ont diminué ; et d'autre part, en France, Macron a remporté les deux tours des élections présidentielles en 2017. Toutefois, nous devons nous demander quel impact ces actions pourraient avoir à l'avenir (Bocquer, 2022). Si, par exemple, le processus sécessionniste revenait à la charge ou si les élections françaises étaient extrêmement serrées.

Toutefois, nous devons maintenant nous tourner vers l'avenir et investir dans de nouvelles infrastructures plus avancées pour mettre fin à ce type d'ingérences. L'imparable développement des cybercapacités russes -douées d'indétectables malwares- met en évidence la nécessité de prendre des mesures telles que « la défense coordonnée entre les secteurs publique et privé » ou « la mise en place d'un système de partage d'information concernant les menaces cybernétiques » (Wolff, 2022). Toute l'infrastructure de l'État doit être protégée en tant que telle, y compris tous les éléments d'un système électoral (Grunemwald, 2018). En bref, les cybercapacités de l'Occident ne peuvent pas continuer à être sous-développées par rapport à celles d'autres États comme la Russie car cela leur permet de profiter de ce vide. Ceci est rendu encore plus clair par les mots de Thomas

Rid: « Russia *tested the red lines of the West, and the result of the test was that there are no red lines yet"* (In Greenberg, 2020).

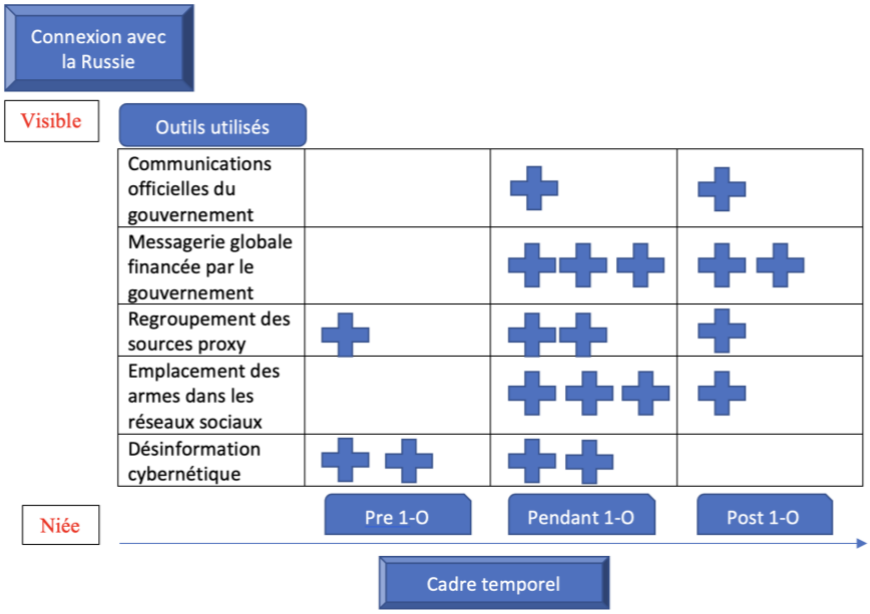
De plus, il est intéressant de mentionner que des lois régissant le cyberespace doivent être développées davantage pour établir un peu d'ordre dans la nébuleuse qu'incarne le cyberespace. À cet égard, les plus récentes avancées de l'UE par rapport à la régulation du monde en ligne, telles que le *fact-checking* ou les *codes de conduite volontaires* pour des plateformes comme Facebook, sont très bénéfiques (Bocquer, 2022). En effet, réglementer ces sujets par la loi permet non seulement de sensibiliser mais aussi de s'attaquer au problème du paternité des cyber-attaques et d'impunité.

Finalement, il convient de rappeler que la polarisation ou le sentiment de malaise au sein d'un État ne sont pas créés, mais peuvent être alimentés par des cyber-attaques (Wolff, 2022). Et suivant l'analyse des cas nous pouvons faire la conclusion suivante : plus il y a de tension ou de polarisation dans une société, plus cette dernière est susceptible de succomber aux effets d'une cyber-attaque. C'est pourquoi, d'un point de vue comparatif, l'impact a été plus important en Espagne qu'en France.

Finalement et concernant le futur de ce sujet, le défi de l'attribution et de l'analyse critique de leur impact réel sur les démocraties d'aujourd'hui ne peut être relevé que par une surveillance accrue des processus électoraux et une protection renforcée de la structure institutionnelle de l'État (Wolff, 2022). La grande difficulté des tests d'hypothèses liés aux cyber-attaques est et restera un obstacle à la recherche dans ce domaine, du moins pour l'instant. Néanmoins, en suivant les événements au jour le jour et en les comparant avec les niveaux de cyberactivité en provenance de Russie, on pourrait tirer des conclusions plus précises.

7. ANNEXE

Annexe I : Tableau de différenciation des actions russes avant, pendant et après le référendum du 1-O et son explication détaillé.



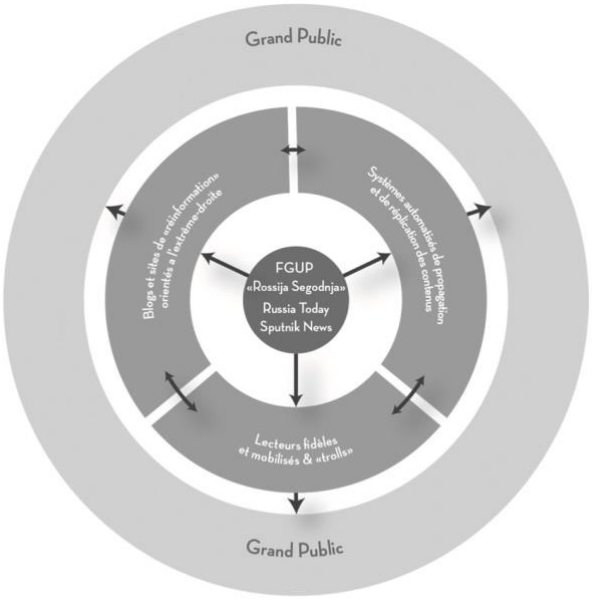
Krah Ripoll, V. (2021). La guerra no lineal contra Occidente a través de un estudio de caso de la injerencia rusa en el conflicto independentista catalán. [Dissertation]. *Repositorium Comillas*. (p. 53). Madrid: Universidad Pontificia Comillas.

Ci-dessous on fournit une définition détaillée des termes figurant dans ce tableau (Krah, 2021) :

- Communications officielles du gouvernement : Déclarations officielles du Kremlin, ses fonctionnaires ou des médias contrôlés par l'État russe. Un exemple a été la déclaration de son ministre des Affaires Étrangères, Lavrov, qui a assuré que le conflit catalan était circonscrit aux affaires internes de l'État espagnol.
- Regroupement des sources proxy : Contiennent les médias alignés sur la Russie. C'est-à-dire, catalyseurs de la rhétorique russe à l'extérieur.
- Messagerie financée par l'État russe : Moyens de communication financés par la Russie et avec une sphère d'influence à l'étranger.

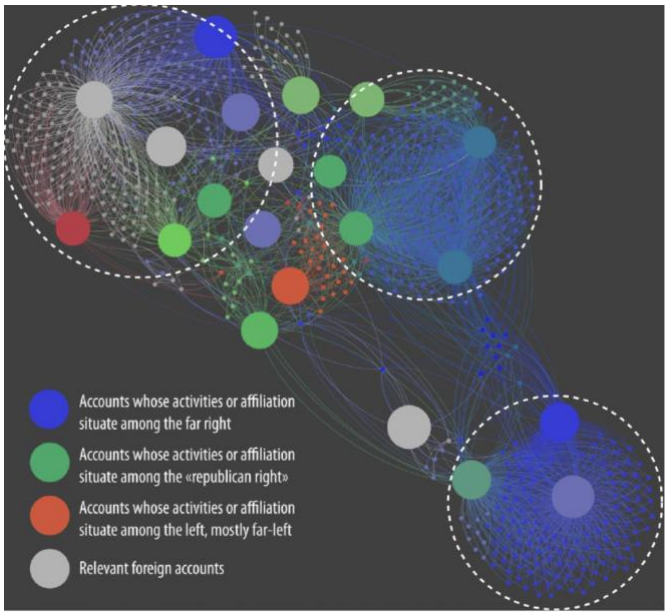
- Emplacement des armes dans les réseaux sociaux : Campagnes visant à miner la foi dans les institutions et à fomenter la polarisation et le discord civil.
- Désinformation cybernétique : Fait allusion au piratage et à la publication d'information sensible, clonage de site web et perturbation de médias avec objectivité.

Annexe II : Schéma de propagation de contenus et matériaux informationnels.



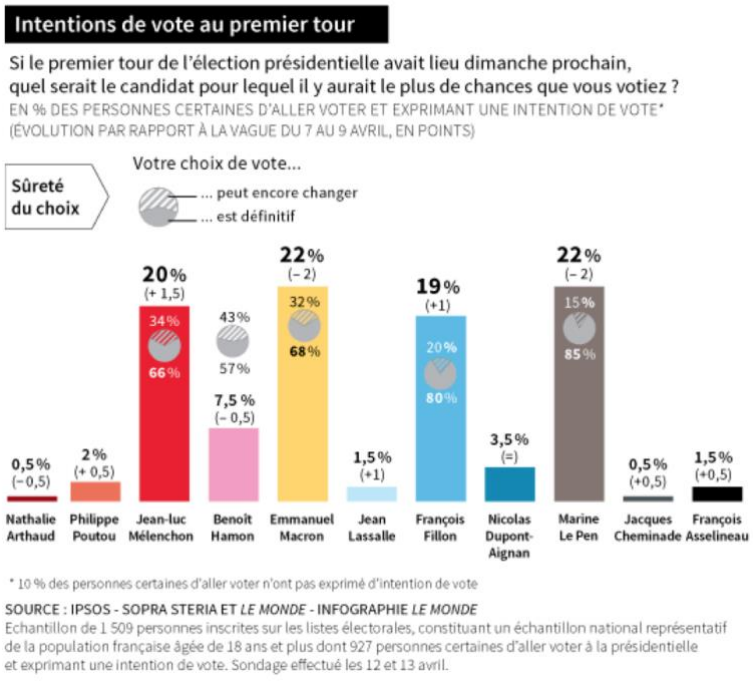
Limonier, K., & Gérard, C. (2017). Guerre hybride russe dans le cyberespace. *Hérodote,* (166-167), 153.

Annexe III : Carte de la twittersphère pro-russe



Pétiniaud, L., & Limonier, K. (2018), Cartographier le Cyberespace : Le cas des actions informationnelles russes en France. *Les Champs De Mar*, (3), 320.

Annexe IV : Enquête complémentaire sur les intentions de vote des 12 et 13 avril



Courtois, G. (2017). Sondage présidentielle 2017 : Le Pen, Macron, Mélenchon, Fillon au coude-à-coude dans les intentions de vote. *Le Monde*. Last retrieved on the 5th of January 2022 from https://www.lemonde.fr/election-presidentielle-2017/article/2017/04/14/presidentielle-le-pen-macron-melenchon-fillon-au-coude-a-coude_5111191_4854003.html

Annexe V : Différents sondages complémentaires sur les intentions de vote dans les jours précédents au premier tour.

DATE	POLLSTER	MACRON	LE PEN	FILLON	MÉLENCHON	HAMON	SAMPLE*
Apr 21–21	Odoxa	24.5%	23%	19%	19%	7.5%	953
Apr 18–21	Ifop-Fiducial	24.5%	22.5%	19.5%	18.5%	7%	2,823
Apr 17–21	OpinionWay	23%	22%	21%	18%	8%	1,500
Apr 19–20	Ipsos Sopra-Steria	24%	22%	19%	19%	7.5%	2,048

Source: FT Research

Wisniewska, A., Locke, C., Nevitt, C., & Rininsland, A. (2017, 7 May). French presidential poll tracker 2017. *The Financial Times*. Last Retrieved on the 16th of May 2022 from https://ig.ft.com/sites/france-election/polls/

Annexe VI : Différents sondages complémentaires sur les intentions de vote dans les jours précédents au deuxième tour.

DATE	POLLSTER	LE PEN	MACRON	SAMPLE*
May 5–5	Ipsos	37%	63%	8,200
May 2–5	Ifop-Fiducial	37%	63%	1,861
May 2–5	Harris Interactive	38%	62%	4,619
May 4–4	Odoxa	38%	62%	959
Apr 28–4	Opinionway	38%	62%	1,500
May 4–4	Ipsos	38.5%	61.5%	2,632

Wisniewska, A., Locke, C., Nevitt, C., & Rininsland, A. (2017, 7 May). French presidential poll tracker 2017. *The Financial Times*. Last Retrieved on the 16th of May 2022 from https://ig.ft.com/sites/france-election/polls/

Annexe VII : Transcription de l'entretien à Josephine Wolff, professeur associé de politique de cybersécurité à la Tufts Fletcher School. Les questions ont été posées par e-mail, et voici sa transcription exacte en anglais.

- « ***If a cyberattack is perpetrated against a state's structure in a major event like a referendum or a national election, to what extent do you think that the result/outcome could be altered?***

  Results certainly could be altered in this way though fortunately we haven't seen any clear examples of this yet.
- ***If Marine le Pen won the elections in France, do you believe it would have an impact in the European Union? If yes, how and why?***

  I'm afraid this is outside my area of expertise in cybersecurity policy.
- ***How do you think international politics (in particular European politics) would be affected if Catalonia separated from Spain?***

  Again, this is outside my area of expertise. I'm not an expert in European politics.
- ***To what extent do you believe Western populations can be politically manipulated or biased due to cyberattacks perpetrated in the media?***

  We know misinformation is a serious problem but we have little good data on its actual impact, but it does seem to have some potentially significant consequences.
- ***To what extent do you believe Western populations can be politically polarized due to cyberattacks perpetrated in the media?***

  I think to a large extent it can exacerbate existing polarization but probably not create that polarization.
- ***To what degree do you think a State can or should be held accountable for having perpetrated cyberattacks against another State?***

  It depends on the nature and consequences of the attack but attacks on critical infrastructure with significant impacts should have consequences for the perpetrators.
- ***In your opinion, what measures can be taken at the core of a State to avoid cyberattacks in important events like national elections?***

  Investment in critical infrastructure protections, information sharing about threat indicators, and coordinated defense across the public and private sectors».

8. BIBLIOGRAPHIE

- DOCUMENTS OFFICIELS

- Connel, M.; Vogler, S. (2016). Russia´s Approach to Cyber Warfare. *Center for Naval Analyses (CNA).* Last Retrieved on the 30th of December 2021 from https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf
- David, S – US General Rapporteur, NATO Parliamentary Assembly. (2018). *Russian Meddling in Elections and Referenda in the Alliance* (No 181). Last retrieved on 31st October 2021 from https://www.nato-pa.int/download-file?filename=/sites/default/files/2018-11/181%20STC%2018%20E%20fin%20-%20RUSSIAN%20MEDDLING%20-%20DAVIS%20REPORT.pdf
- Jeangène Vilmer, J. (2019). The "Macron-leaks" Operation: A post-mortem. *Atlantic Council*. Last Retrieved on the 16th of May 2022 from https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf
- Rassemblement National (2017). 144 engagements présidentiels. Last Retrieved on the 28th of March 2022 from https://rassemblementnational.fr/pdf/144-engagements.pdf
- Parlement Européen. (2021). *Quelles sont les causes des relations tendues entre l'UE et la Russie? : Actualité: Parlement Européen*. Quelles sont les causes des relations tendues entre l'UE et la Russie ? | Actualité | Parlement Européen. Last retrieved on the 30th of December 2021 from https://www.europarl.europa.eu/news/fr/headlines/world/20210128STO96606/quelles-sont-les-causes-des-relations-tendues-entre-l-ue-et-la-russie
- Union Européen. Traité de l'UE, signed in Maastricht the 7th of February of 1992. Official Diary of the UE L191, 29th of July, p. 4.

- ARTICLES SCIENTIFIQUES

- Arteaga, F. (2018). Las amenazas de nueva generación para las empresas. *Real Instituto Elcano*. Last retrieved on the 11th of October 2021, from http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/comentario-arteaga-amenazas-nueva-generacion-para-empresas

- Baezner, M. (2018). Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict. *Zürich: Center for Security Studies*. Last retrieved on the 9th of November 2021, from https://www.researchgate.net/publication/322364443_Cyber_and_Information_warfare_in_the_Ukrainian_conflict#pfd
- Barbet Porta, B. (2020). Encuesta sobre polarización y convivencia en Cataluña 2020. *ICIP*. Last Retrieved on the 13th of May 2022 from https://www.icip.cat/wp-content/uploads/2021/01/informes_2020-17_cas_compressed.pdf
- Boelaert, J., Michon, S., & Ollion, É. (2018). Le temps des élites : Ouverture politique et fermeture sociale à l'Asamblée Nationale en 2017. *Revue Française De Science Politique, 68*, 777-802.
- Chausovsky, E. (2018). How Russia makes power plays in European politics. *On Geopolitics*, 1.
- Chu, Z., Gianvecchio, S., Wang, H., & Jajodia, S. (2010). Who is tweeting on Twitter: human, bot, or cyborg?. In *Association for Computing Machinery* (pp. 21–30). New York: Association for Computing Machinery. Last Retrieved on the 24th of November 2021, from https://dl.acm.org/doi/abs/10.1145/1920261.1920265
- Douzet, F. (2014). La géopolitique pour comprendre le cyber espace. *Hérodote*, (152-153), 3-21.
- Emmott, R. (2017). Spain sees Russian interference in Catalonia separatist vote. *Reuters*. Last retrieved on the 30th of October 2021, from https://www.reuters.com/article/us-spain-politics-catalonia-russia-idUSKBN1DD20Y
- Firoozabadi, J. D., & Ashkezari, M. Z. (2016, May). Neo-classical realism in International Relations. *Asian Social Science, 12 (6)*, 95-99.
- Fonfría, A., & Duch-Brown, N. (2020, September 14). Ciberseguridad económica. *Real Instituto Elcano*. Last retrieved on the 14th of November 2021, from http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GL

OBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari105-2020-fonfria-duch-brown-ciberseguridad-economica

- Iosifidis, P., y Wheeler, M. (2018). Modern political communication and web 2.0 in representative democracies. *Javnost-The public, 25*(1-2), págs. 110-118. https://doi.org/10.1080/13183222.2018.1418962
- Joseph, J. (2014). Realism and Neorealism in International Relations Theory. *The Encyclopedia of Political Thought*, M.T. Gibbons. (Ed.). Last Retrieved on the 20th of November 2020 from https://doi.org/10.1002/9781118474396.wbept0864
- Kadlecová, L. (2018). State Reponsability in the Cyber Age: The Course towards Indirect Evidence. *Mezinarodni Vztahy*, *53* (4), 35-46.
- Kamiya, S., Kang, J., Kim, J., Milidonis, A., & Stulz, R. M. (2018). What is the impact of successful cyberattacks on target firms? *NBER Working Paper Series*, 1-30. Last Retrieved on the 25th of May 2022 from Retrieved from https://www.embroker.com/blog/cyber-attack-statistics/
- Kausch, K. (2018). Cibergeopolítica y estabilidad en Oriente Próximo. *Política Exterior, 32*(181), 106-114.
- Kshetri, N. (2016). Cybersecurity in Russia. *The Quest to Cyber Superiority*, (pp. 211-221). North Carolina: University of North Carolina.
- Lewis, J. A. (2018). Economic Impact of Cybercrime: At $ 600 Billion & Counting - No Slowing Down. *Center for Strategic and International Studies*. Last Retrieved on the 23rd of November 2021, from https://www.csis.org/analysis/economic-impact-cybercrime
- Limonier, K., & Gérard, C. (2017). Guerre hybride russe dans le cyberespace. *Hérodote*, (166-167), 145-163.
- Lo, B. (2018). Chutzpah and Realism: Vladimir Putin and the Making of Russian Foreign Policy. *Russie. Nei. Visions, No. 108, Ifri*. Last Retrived on the 30th of November from https://www.ifri.org/sites/default/files/atoms/files/bobo_lo_chutzpah_and_realism_2018.pdf
- López, O., Carlos, & Fenoll, V. (2020). La polarización mediática en el proceso de independencia en Cataluña. estudio comparativo del tratamiento en RT. *Mediterranean Journal of Communication, 11*(1), 261-272.

- Masip, P., Guau, J., & Ruiz-Caballero, C. (2020). Percepciones sobre medios de comunicación y desinformación: Ideología y polarización en el sistema mediático español. *Profesional De La Información*, *29*(5), 1-13.
- Medina, L. (2018). Cataluña: ¿una sociedad dividida por la mitad? El efecto del contexto entre los no nacionalistas. *Quaderns De L'ICPS*, (16), 1-10.
- Milosevich-Juaristi, M. (2017 a). El poder de la influencia rusa: la desinformación. *Real Instituto Elcano*. Last retrieved on the 31st of October 2021 from http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari7-2017-milosevichjuaristi-poder-influencia-rusa-desinformacion
- Milosevich-Juaristi, M. (2017 b). La "combinación", instrumento de guerra de información de Rusia en Cataluña. *Real Instituto Elcano*. Last retrieved on the 31st of October 2021 from http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari86-2017-milosevichjuaristi-combinacion-instrumento-guerra-informacion-rusia-cataluna
- Molina, I., & Martín, N. (2019). La crisis catalana y la influencia de España en Bruselas. *Real Instituto Elcano.* Last Retrieved on the 15th of May 2022 from https://www.realinstitutoelcano.org/analisis/la-crisis-catalana-y-la-influencia-de-espana-en-bruselas/
- Pally, Y.A (2020). Cyberattacks and disinformation campaigns. *Journal of Social Political Sciences, 1*(3), 195.
- Pasquier, R. (2004). Les régions et les styles nationaux de politiques territoriales. *La capacité politique des régions*. 83-126. Rennes : Presses Universitaires de Rennes.
- Pavlova, E., & Romanova, T. (2012). Towards neoclassical realist thinking in Russia?. *Neo-classical realism in European Politics: Bringing power Back In* (pp. 234-254). Manchester: Manchester University Press.
- Pétiniaud, L., & Limonier, K. (2018), Cartographier le Cyberespace : Le cas des actions informationnelles russes en France. *Les Champs De Mar*, (3), 317-326.
- Pocheptsov, G. (2017). *Каталонская спецоперация: Последствия информационных атак как урок для украины*. (pp. 1-8). Mariupol State

University. Last Retrived on the 27th of March 202 from https://www.researchgate.net/publication/321831207_Katalonskaa_specoperacia_posledstvia_informacionnyh_atak_kak_urok_dla_Ukrainy

- Polyakova, A. (2017). The Kremlin's Trojan Horses 2.0. *Atlantic Council.* Last Retrieved on the 30th of October 2021 from http://www.jstor.com/stable/resrep16776.3

- Polyakova, A., & Boyer, S. P. (2018). The future of political warfare: Russia, the west, and the coming age of global digital competition. *Brookings Institution*, 1-18.

- Prissette, N. (2017). *Emmanuel Macron : Le président inattendu.* Paris: First-Gründ, Paris. Last Retrieved on the 15th of May 2022 from https://books.google.be/books?hl=en&lr=&id=tjwkDwAAQBAJ&oi=fnd&pg=PT4&dq=impact+des+cyberattaques+contre+Macron+2017&ots=OFDgIQgoq1&sig=4omqSgW3OTsWk1cMm-mp44snfj0&redir_esc=y#v=onepage&q&f=false
- Real Instituto Elcano. (2019). El conflicto independentista español. Last Retrieved on the 26th of March 2022 from https://www.realinstitutoelcano.org/documento-de-trabajo/el-conflicto-independentista-en-cataluna/
- Roman, N., Wanta, W., y Buniak, I. (2017). Information wars: Eastern Ukraine military conflict coverage in the Russian, Ukrainian and U.S. newscasts. *International Communication Gazette, 79*(4), 357–378. DOI: 10.1177/1748048516682138
- Romanova, T. A. (2012). Neoclassical Realism and Today's Russia. *Russia in Global Affairs*, (3) Last Retrieved on the 30th of November 2021 from https://eng.globalaffairs.ru/articles/neoclassical-realism-and-todays-russia/
- Ross Smith, N. (2018, Apr 1,). Can neoclassical realism become a genuine theory of International Relations?. *Journal of Politics, 80*, 742-749.

- Serra, M., Ubasart González, G., & Martí i Puig, S. (2018). Cataluña y la triple crisis española. *Nueva Sociedad: Democracia Y Política En América Latina*, (273), 22-32. ISSN: 0251-3552.

- Silvestre Cabrera, M. (2020). Valores en la era de la incertidumbre: Individualismos y solidaridades. Quinta encuesta europea de valores en su aplicación a España. [Abstract]. *Investigación Y Debate,* (293).
- Snegovaya, M. (2021). Fellow travelers or trojan horses? Similarities across pro-Russian parties' electorates in Europe. *Party Politics, 20*(10), 1-10.
- Soutou, G. (2004). L'identité de l'Europe du point de vue de l'historien. *Outre Terre,* (7), 31-42.
- Surowiec, P. (2017). Post-truth soft power: Changing facets of propaganda, kompromat, and democracy. *Georgetown Journal of International Affairs, 18*(3), 21-27.
- Teruel Rodríguez, L. (2013). El posicionamiento editorial de la prensa española sobre la polarización política. En Sanders, Capdevila & Gurrionero (coords.). *Estudios De Comunicación Política*, (pp. 169-191). Málaga: Tecnos.
- Vilanova, P. (2008). Espagne, trente ans de démocratie : Notes pour un bilan. *Pouvoirs,* (124), 5-18.
- Wieclawski, J. (2011, Contemporary realism and the foreign policy of the Russian Federation. *International Journal of Business and Social Science, 2*, 170-179.

- MÉMOIRES DE FIN D'ÉTUDES, THÈSES DE DOCTORAT

- Krah Ripoll, V. (2021). La guerra no lineal contra Occidente a través de un estudio de caso de la injerencia rusa en el conflicto independentista catalán. [Dissertation]. *Repositorium Comillas*. (pp. 1-60). Madrid: Universidad Pontificia Comillas.
- Martínez Jiménez, C. (2015). El uso de ciberataques como herramienta de relaciones internacionales por parte de los actores estatales: Los casos de Estados Unidos y Rusia. [Dissertation]. *Repositorium Comillas*. (pp. 30-37). Madrid: Universidad Pontificia Comillas.
- Medvedev, S. (2015). *Offense-defense theory analysis of Russian cyber capability* [Disertación doctoral, Naval Postgraduate School]. The NPS Theses and Dissertations. Institutional Archive. https://calhoun.nps.edu/handle/10945/45225

- DOCUMENTS INTERNET

- Internet World Stats (2022). *Internet Usage Statistics. The Internet Big Picture. World Internet Users and 2020 Population Stats*. Last Retrieved on the 3rd of November 2021 from https://www.internetworldstats.com/stats.htm.

- IPSOS (2021). *Global Trustworthiness Index 2021*. Last Retrieved on the 17th May 2022 from https://www.ipsos.com/sites/default/files/ct/news/documents/2021-10/Global-trustworthiness-index-2021.pdf
- Larousse. *Tension*. Last Retrieved on the 13th of May 2022, from https://www.larousse.fr/dictionnaires/francais/tension/77330
- Ministère de l'Intérieur. (2017). *Résultat de l'élection présidentielle 2017*. Last Retrieved on the 28th of May 2022 from https://www.interieur.gouv.fr/Elections/Les-resultats/Presidentielles/elecresult__presidentielle-2017/(path)/presidentielle-2017/FE.html
- RT. [@RT_com]. (2nd of October 2017). [Tweet]. *#Catalan citizens won the right to statehood" – regional president*. Twitter. Last Retrieved on the 2nd of February 2022 from https://twitter.com/rt_com/status/914620944957759488?ref_src=twsrc%5Etfw
- *RTVE Noticias*. RTVE. (n.d.). Last Retrieved on the 24th of November 2021 from https://www.rtve.es/.
- Statista Research Department. (2021). Preliminary results of the Catalan self-determination referendum on October 1st, 2017. Las retrieved on the 3rd of January 2022 from https://www.statista.com/statistics/755833/catalan-self-determination-referendum-results/
- Statista Research Department. (2020). Do you think that the Catalan referendum is an internal affair of Spain or an EU issue?. Last retrieved on the 3rd of January 2022 from https://lb-aps-frontend.statista.com/statistics/757412/opinion-on-catalan-referendum-in-italy/

- PRESSE HEBDOMADAIRE

- Greenberg, A. (2020, October 19). *Wired*. Last Retrieved on the 22nd of November 2021, from https://www.wired.com/story/us-indicts-sandworm-hackers-russia-cyberwar-unit/
- Hennessey, S. (2017). Deterring cyberattacks: How to reduce vulnerability. *Foreign Affairs*. Last Retrieved on the 3rd of November 2021

from https://www.foreignaffairs.com/reviews/review-essay/2017-10-16/deterring-cyberattacks

- Inglis, C., & Krejsa, H. (2022). The cyber social contract. *Foreign Affairs. Last* Retrieved on the 26th of March 2022 from https://www.foreignaffairs.com/articles/united-states/2022-02-21/cyber-social-contract?utm_medium=newsletters&utm_source=fatoday&utm_campaign=The%20Cyber%20Social%20Contract&utm_content=20220221&utm_term=FA%20Today%20-%20112017

- PRESSE QUOTIDIENNE

- AFP. (2022). Le Parti de Macron la République en marche change de nom et devient "Renaissance". *Le Soir*. Last retrieved on the 13th of May 2022 from https://www.lesoir.be/440410/article/2022-05-05/le-parti-de-macron-la-republique-en-marche-change-de-nom-et-devient-renaissance
- Alandete, D. (2017 a). La maquinaria de injerencias rusa penetra en la crisis catalana. *El País*. Last Retrieved on the 23rd of November 2021, from https://elpais.com/politica/2017/09/22/actualidad/1506101626_670033.html
- Alandete, D. (2017 b). Putin alienta la independencia con un enviado a Cataluña. *El País*. Last Retrieved on the 23rd of May 2022 from https://elpais.com/politica/2017/10/25/actualidad/1508958307_955473.html
- Hernández, H. (2020). Analyse de la désinformation en Europe (IV). *Atalayar*. Last Retrieved on the 28th of May 2022 from https://atalayar.com/fr/content/analyse-de-la-d%C3%A9sinformation-en-europe-iv
- Auchard, E., & Felix, B. (2017). French candidate Macron claims massive hack as emails leaked. *REUTERS*. Last Retrieved on the 16th of May 2022 from https://www.reuters.com/article/us-france-election-macron-leaks-idUSKBN1812AZ
- Barber, T. (2017). The Catalan crisis poses a threat to the European order. *The Financial Times*. Last retrieved on the 3rd of January from https://www.ft.com/content/b31c20f8-a9bb-11e7-ab55-27219df83c97

- BBC Mundo. (2017). 4 casos de noticias falsas que intoxicaron el debate sobre la independencia de Cataluña de España. Last Retrieved on the 23rd of May 2022 from https://www.bbc.com/mundo/noticias-internacional-41703119
- Benito, R. (2017). "La opinión pública europea sobre Cataluña ha cambiado". *El Mundo*. Last retrieved on the 4th of January 2022 from https://www.elmundo.es/espana/2017/11/11/5a0617aae2704e8b578b4663.html
- Casal, L. (2022). Una red de ultraderecha une a Vox con los oligarcas rusos de Putin a través de HazteOir y CitizenGo. *El Español*. Last Retrieved on the 26th of March 2022 from https://www.elespanol.com/reportajes/20220319/ultraderecha-vox-oligarcas-putin-traves-hazteoir-citizengo/658184665_0.html
- Catalans strike over violent crackdown on independence referendum. (2017). France 24h. Last retrieved on the 4th of January 2022 from https://www.france24.com/en/20171003-catalans-catalonia-strike-independence-referendum-police-crackdown-violence-spain
- Cattler, D. & Black. D. (2022). The Myth of the Missing Cyberwar. *Foreign Affairs*. Last Retrieved on the 6th of April 2022 from https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar?utm_medium=newsletters&utm_source=fatoday&utm_campaign=The%20Price%20of%20Hegemony&utm_content=20220406&utm_term=FA%20Today%20-%20112017
- Child, D. (2017). Catalonia vote: Social media mirrors street tension. *Al Jazeera*. Last retrieved on the 4th of January 2022 from https://www.aljazeera.com/news/2017/10/1/catalonia-vote-social-media-mirrors-street-tension
- Courtois, G. (2017). Sondage présidentielle 2017 : Le Pen, Macron, Mélenchon, Fillon au coude-à-coude dans les intentions de vote. *Le Monde*. Last retrieved on the 5th of January 2022 from https://www.lemonde.fr/election-presidentielle-2017/article/2017/04/14/presidentielle-le-pen-macron-melenchon-fillon-au-coude-a-coude_5111191_4854003.html
- Dorell, O. (2017). Russia engineered election hacks and meddling in Europe. *USA Today*. Last retrieved on the 3rd of November 2021 from https://eu.usatoday.com/story/news/world/2017/01/09/russia-engineered-election-hacks-europe/96216556/

- Geoffroy, R., & Vaudano, M. (2022). Quels sont les liens de Marine le Pen avec la Russie de Vladimir Poutine?. *Le Monde*. Last Retrieved on the 17th of May 2022 from https://www.lemonde.fr/les-decodeurs/article/2022/04/20/quels-sont-les-liens-de-marine-le-pen-avec-la-russie-de-vladimir-poutine_6122903_4355770.html
- Grunemwald, B. (2018, Mar). Piratage de la démocratie : les processus électoraux peuvent-ils être protégés?. *Les Echos*. Last Retrieved on the 26th of March from https://www.lesechos.fr/idees-debats/cercle/piratage-de-la-democratie-les-processus-electoraux-peuvent-ils-etre-proteges-130933
- Lesaca, J. (2017). Why did Russian social media swarm the digital conversation about Catalan independence? *The Washington Post*. Last Retrieved on the 2nd of November 2021 from https://www.washingtonpost.com/news/monkey-cage/wp/2017/11/22/why-did-russian-social-media-swarm-the-digital-conversation-about-catalan-independence/
- Mazuir, V. (2021). François Fillon et l'affaire des emplois fictifs. *Les Echos*. Last Retrieved on the 15th of May 2022 from https://www.lesechos.fr/politique-societe/politique/francois-fillon-et-laffaire-des-emplois-fictifs-1167582
- Ordaz, P. (2017). El día que los catalanes dejaron de hablarse. El País. Last Retrieved on the 26th of March 2022 from https://elpais.com/politica/2017/12/16/actualidad/1513455966_708321.html
- Palmer, E. (2017). Spain Catalonia: Did Russian "fake news" stir things up?. *BBC*. Last retrieved on the 4th of January 2022 from https://www.bbc.com/news/world-europe-41981539
- Pietralunga, C., Bonnefous, B., & Fayer, O. (2017). Macron-Le Pen : Un débat brutal, désordonné, qui laissera des traces. *Le Monde*. Last Retrieved on the 29th of May 2022 from https://www.lemonde.fr/election-presidentielle-2017/article/2017/05/04/macron-le-pen-un-debat-brutal-desordonne-qui-laissera-des-traces_5121930_4854003.html
- Rankin, J. (2017). Catalan independence: EU experts detect rise in pro-Kremlin false claims. *The Guardian*. Last Retrieved on the 23rd of May 2022 from https://www.theguardian.com/world/2017/nov/13/catalan-independence-eu-experts-detect-rise-in-pro-kremlin-false-claims

- Référendum : Le gouvernement catalan proclame la victoire du "oui" à l'indépendance avec 90% des voix. (2017). *Le Soir*. Last retrieved on the 4th of January 2022 from https://www.lesoir.be/117079/article/2017-10-02/referendum-le-gouvernement-catalan-proclame-la-victoire-du-oui-lindependance
- Tauziac, A. (2017). Présidentielle 2017 : La menace de cyberattaques russes est-elle crédible ?. *Sudouest*. Last Retrieved on the 15th of May 2022, from https://www.sudouest.fr/economie/reseaux-sociaux/presidentielle-2017-la-menace-de-cyberattaques-russes-est-elle-credible-3412551.php
- Viktine, B. (2016). Poutine et Fillon, une amitié géopolitique. *Le Monde*. Last Retrieved on the 18th of May 2022 from https://www.lemonde.fr/election-presidentielle-2017/article/2016/11/22/fillon-et-la-russie-une-relation-profonde-et-ancienne_5035506_4854003.html
- Wisniewska, A., Locke, C., Nevitt, C., & Rininsland, A. (2017, 7 May). French presidential poll tracker 2017. *The Financial Times*. Last Retrieved on the 16th of May 2022 from https://ig.ft.com/sites/france-election/polls/