De la prédiction à la détection d'évènements : L'analyse des mégadonnées au service du renseignement de sources ouvertes

Fanch Francis

Université de Lille

École doctorale Sciences de l'Homme et de la Société

Groupe d'Études et de Recherche Interdisciplinaire en Information et Communication

De la prédiction à la détection d'évènements

L'analyse des mégadonnées au service du renseignement de sources ouvertes

Par Fanch FRANCIS

Thèse de doctorat de sciences de l'information et de la communication

Dirigée par Laurence Favier

Présentée et soutenue publiquement le 8 novembre 2019

Devant un jury composé de :

Laurence Favier, professeur des universités, Université de Lille, directeur de thèse
Widad, Mustafa El Hadi, professeur des universités, Université de Lille, présidente du jury
Fabrice Papy, professeur des universités, Université de Lorraine, rapporteur
Madjid Ihadjadene, professeur des universités, Université de Paris 8, rapporteur
Jean-Claude Bessez, lieutenant-colonel, docteur en civilisation britannique, examinateur
Bernard L'Hostis, représentant de la direction générale de l'armement, invité

Je dédicace cette thèse aux officiers mariniers et sous-officiers des forces armées françaises et plus particulièrement au personnel du renseignement.

Titre : De la prédiction à la détection, l'analyse des mégadonnées au service du renseignement de sources ouvertes.

Résumé :

Comprendre les dynamiques d'un conflit pour en anticiper les évolutions est d'un intérêt majeur pour le renseignement militaire de sources ouvertes (ROSO) et le renseignement policier, notamment dans le cadre de l'Intelligence Led Policing. Si l'ambition de vouloir prédire les évènements d'un conflit n'est pas réaliste, celui de les détecter est un objectif important et réalisable. Les sciences humaines et sociales particulièrement les sciences de l'information et de la communication combinées à la science des données et des documents permettent d'exploiter les réseaux sociaux numériques de manière à faire de la détection et du suivi d'évènement un objectif et une méthode plus adaptées que le "protest event analysis" au contexte des guerres modernes et de la société connectée. Cela nécessite en même temps de rénover le cycle du renseignement.

En nous basant sur les données du réseau social Twitter, recueillies pendant la crise ukrainienne, cette thèse montre la pertinence de détection et de suivi de conflit au moyen de notre méthode DETEVEN. Cette méthode permet non seulement d'identifier les évènements pertinents dans un conflit, mais en facilite aussi leur suivi et interprétation. Elle repose sur une détection d'anomalie statistique, et une adaptation du "protest event analysis" aux médias sociaux. Notre méthode s'avère particulièrement efficace sur ce que nous définissons comme des théâtres d'opération connectés (TOC) caractéristiques des nouveaux contextes de guerre hybride et sur des opérations de désinformation ou d'influence. Ces évènements détectés ont été exploités de façon analytique au moyen d'une plateforme conçue pour un analyste, permettant une visualisation efficace des données. Dans une situation de crise, plus encore dans une "guerre de mouvement social", où chaque utilisateur devient de fait un capteur social, la maîtrise de l'information est un enjeu stratégique. Cette thèse montre alors comment cette maîtrise de l'information constitue un important enjeu à titre individuel comme collectif.

Mots clefs :

Renseignement de source ouverte, réseaux sociaux numériques, maîtrise de l'information, intelligence artificielle, Web sémantique, données massives, détection d'événements, maîtrise de l'information, police guidée par le renseignement, protest event analysis.

Title : From Prediction to Detection, Big Data Analytics for Open Source Intelligence.

Abstract :

Understanding the dynamics of a conflict in order to anticipate its evolution is of major interest for military intelligence and police intelligence, particularly in the context of Intelligence Led Policing. If the ambition to predict events in a conflict is not realistic, to detect them is an important and achievable objective. The human and social sciences, particularly the information and communication sciences combined with the science of data and documents, make it possible to exploit digital social networks in such a way as to make event detection and monitoring a more appropriate objective and method than standard "protest event analysis" in the context of modern wars and the connected society. At the same time, this requires a renewed intelligence cycle.

Based on data from the social network Twitter, collected during the Ukrainian crisis, this thesis shows the relevance of conflict detection and monitoring using our DETEVEN method. This method not only identifies relevant events in a conflict, but also facilitates their monitoring and interpretation. It is based on the detection of statistical anomalies and the adaptation of protest event analysis to social media. Our method is particularly effective on what we define as connected theatres of operation (CTOs) characteristic of new hybrid warfare contexts and on operations of

misinformation or influence. These detected events were analytically exploited using a platform designed for an analyst, allowing effective data visualization. In a crisis situation, especially in a "social movement war", where each user becomes a de facto social sensor, information control is a strategic issue. This thesis then shows how information literacy is an important issue for individuals and groups.

Keywords :
Open Source Intelligence, Digital Social Networks, Information Literacy, Artificial Intelligence, Semantic Web, Big Data, Event Detection, information literacy, intelligence-led policing protest event analysis.

Remerciements

Liste des principales abréviations

ALA : American Library Association

APAVIA : Anomalies pouvant avoir valeur d'indices d'alertes

API : Application Programming Interface

ARPANET : Advanced Research Projects Agency Network

ARTEMIS : Architecture de traitement et d'exploitation massive de l'information multi-source

ASL : Armée Syrienne Libre

CAPS : Centre d'analyse, de prévision et de stratégie du ministère de l'Europe et des Affaires étrangères

CIAE : Centre interarmées des actions sur l'environnement

CICDE : Centre interarmées de concepts, de doctrines et d'expérimentations

CML : Center for Media Literacy

CNESCO : Conseil national d'évaluation du système scolaire

CSV : Coma separated value

C4ISR : Commandement, contrôle, communication, informatique, renseignement, surveillance et reconnaissance

C4ISTAR : Commandement, contrôle, communication, informatique, renseignement, surveillance, acquisition de cible et reconnaissance

DARPA : Defense Advanced Research Projects Agency

DETEVEN : Détection d'évènement

DGA : Direction Générale de l'Armement

DTRA : Defense threat reduction agency

EEI : Engins explosifs improvisés

EIIL : État Islamique

EIREL : École interarmées du renseignement et des études linguistiques

EMI : Education aux médias et à l'information

FAI : Fournisseur d'accès à internet

FNAEG : Fichier national des empreintes génétiques

FOAF : Friend of a Friend

HLEG : High Level Expert Group

IARPA : Intelligence Advanced Research Projects Activity

ILP : Intelligence led policing

IM : Influence militaire

IOT : Internet des objets

IRSEM : Institut de recherche stratégique de l'École militaire

ISN : International Relations and Security Networ

JSON : JavaScript Object Notation

LASR de SAS : Plate-forme fournissant un environnement multi-utilisateurs sécurisé permettant un accès simultané aux données chargées en mémoire

LPM : Loi de programmation militaire

ML : Machine Learning

MPEDS : Machine-Learning Protest Event Data System

NIJ : National Institute of Justice

NTIC : Nouvelles technologies de l'information et de la communication

ODCS : Organisation de la Défense Civile Syrienne

ONU : Organisation des nations unies

OSCE : Organisation pour la sécurité et la coopération en Europe

OSINT : Open source intelligence

OTAN : Organisation du traité de l'Atlantique Nord

PEA : Protest Event Analysis

RDF : Resource Description Framework

ROHUM : Renseignement d'origine humaine

ROSO : Renseignement de sources ouvertes

RSF : Reporter Sans Frontières

SCIOC : Semanticly interlinked online communities

SEO : Search Engine Optimization

SHS : Sciences humaines et sociales

SIC : Sciences de l'information et de la communication

SKOS : Simple knowledge organization system

SPARQL : Language de requête pour le RDF

SSL : Strategic Subject List

TDT : Topic Detection and Tracking

TOC : Théâtre d’opération connecté

UE : Union Européenne

UGC : User Generated Content

UNESCO : Organisation des Nations unies pour l'éducation, la science et la culture

VK : Vkontakte

W3C : World Wide Web Consortium


AFP/Getty Images

Sommaire

INTRODUCTION GÉNÉRALE

« Ce sont les évènements qui commandent aux hommes, et non les hommes aux évènements. »
(Histoires, Hérodote, 445 av. J.-C.)

Parmi les outils de recueil du renseignement militaire, les sources ouvertes tiennent une place particulière. Considérées comme peu fiables pour certains, indispensables pour d'autres, leur usage est l'objet de nombreux questionnements. Cependant, notre expérience professionnelle nous a amené à constater que les sources ouvertes font partie intégrante du processus de création de renseignements en particulier en ce qui concerne l'analyse des conflits étrangers. En effet, il n'est pas possible d'avoir des capteurs confidentiels (humains ou techniques) partout, alors qu'il est tout à fait aisé de recueillir en masse ce qui se dit sur l'internet. Il s'agit ici de l'intérêt majeur du renseignement de sources ouvertes. Chaque utilisateur d'internet et plus particulièrement des réseaux sociaux devient un capteur et un indicateur d'alerte en ayant un rôle à la fois passif et actif. En plus de leur couverture mondiale, ces *capteurs sociaux* ne coûtent rien à mettre en œuvre et ne représentent aucun risque de compromission à l'inverse de leurs pendants humains et techniques. Ces capteurs sociaux ne sont pas sans défaut, et comme tout outil de recueil, leurs biais doivent être pris en compte. Cependant leur capacité se révèle sans aucun égal dans les situations qui impliquent des groupes telles que les mouvements sociaux.

Dans le domaine du renseignement de situation, comprendre un mouvement social ne peut se limiter à en observer les faits à distance au travers de médias numériques. Ne pas être en mesure d'en saisir les dynamiques entraînerait une impossibilité d'en estimer les impacts et évolutions possibles. Or il s'agit là d'une des fonctions essentielles de l'analyste en renseignement. À ce titre, il nous paraît essentiel dans ce premier chapitre de nous inscrire dans le domaine des sciences humaines et sociales (SHS) pour l'étude des mouvements sociaux et plus particulièrement dans les situations de conflit afin de montrer comment les mécanismes identifiés en SHS peuvent servir de base de modélisation de l'intelligence artificielle.

L'exploitation des données de masse est une problématique constante, le volume de données produites dépassant les capacités d'exploitation. Alors que de nombreux programmes industriels et d'État font une priorité du déploiement de l'intelligence artificielle dans la valorisation de la donnée, notamment pour le renseignement militaire, il n'existe pas de consensus sur les modèles que celle-ci devra mettre en œuvre. Ainsi, il nous paraît inadapté de

reprendre des modèles de prédiction de comportement individuel issus du domaine commercial, médical ou culturel pour soutenir l'analyse de situation de conflit.

Selon la stratégie nationale du renseignement de juillet 2019, le renseignement : « *recouvre l'ensemble des informations et faits révélés et analysés par le travail des services dans le but de prévenir les atteintes aux intérêts de la Nation, de protéger les personnes, les biens et les institutions et de défendre et promouvoir les intérêts de la France.* » (SGDSN, 2019). Cette définition par le but est somme toute classique. La véritable nouveauté de cette mise à jour de la stratégie se trouve dans la priorisation des enjeux. En effet, si l'enjeu numéro un reste la lutte contre le terrorisme, le deuxième enjeu prioritaire est : « *l'anticipation des crises et des risques de ruptures majeures* » notamment dans le cadre de crises de sécurité intérieure. De là à y voir un résultat direct du mouvement des gilets jaunes, c'est-à-dire ces manifestations contre le gouvernement tous les samedis depuis le mois d'octobre 2018, il n'y a qu'un pas. Cette crise d'ordre public d'ampleur inédite est arrivée comme une véritable surprise pour les gouvernants. À ce titre, la demande est claire, il faut anticiper.

L'anticipation, le fait de devancer l'action, s'accompagne de prévisions, c'est-à-dire d'un processus de détermination de l'évolution d'une situation en se basant sur des faits en cours, voire de prédiction, qui est tout simplement la capacité de voir dans le futur. Ce dernier point a toute l'attention des chercheurs en intelligence artificielle, qu'il s'agisse de domaines aussi variés que le marketing, la météorologie, la santé, la conduite de véhicule ou la compatibilité relationnelle entre humains. Aujourd'hui, les capacités de recueil de l'information et son exploitation au moyen de machines et d'algorithme permettraient de rendre tout prédictible. Il paraît donc normal que les autorités s'attendent à ce que des crises sociétales rentrent dans le domaine de la prédiction.

Dans le cadre de la prédiction des crises, serions-nous déjà arrivés aux limites de l'intelligence artificielle ? Ou plutôt serions-nous en train de nous tromper de mission ? Le moteur principal de l'intelligence artificielle reste le secteur économique. Tant dans le marketing que dans la santé, l'objectif premier de l'intelligence artificielle est de prédire le comportement individuel pour vendre ou fournir à l'individu ce dont il aura envie ou besoin. En clair, il s'agit d'une modélisation du ciblage. Dans le domaine militaire, l'objectif reste le même : cibler l'individu dans la masse. Or, une crise d'ordre public est plus que la somme des individus qui y participent. Si l'on veut anticiper une crise, il ne faut pas s'appuyer sur une mythologie de l'anticipation du comportement individuel, mais appliquer l'intelligence artificielle à l'échelle adéquate qui, pour nous, est l'évènement. Notre recherche porte donc sur la détection d'évènements plutôt

que sur la prédiction de comportement. La crise est une série d'évènements vécus par un groupe d'individus. Ce groupe rapporte sur l'évènement ce qui le rend détectable comme tel.

Évènement, du latin evenire – ex-venire, se traduit par l'issue, le résultat, mais aussi ce qui arrive : « *on assiste à une évolution de la structure sémantique issue du latin : le sens de « résultat* » (qui marque l'accomplissement d'une forme de causalité) tend à s'effacer, l'idée de surgissement, de rupture tend à s'imposer. » (Boisset, 2016). Dans son acception moderne, la notion d'évènement est un fait ou ensemble de faits se distinguant des faits concomitants par sa nature, sa portée, son impact. Un fait peut devenir un évènement, au même titre qu'une donnée peut devenir une information, et une information, un renseignement.

La notion d'évènement implique qu'il soit vécu par des personnes : « *Son arrivée dans le temps (c'est en ce sens qu'il est le point focal autour duquel se déterminent un avant et un après) est immédiatement mise en partage par ceux qui le reçoivent, le voient, en entendent parler, l'annoncent puis le gardent en mémoire. Fabricant et fabriqué, constructeur et construit, il est d'emblée un morceau de temps et d'action mis en morceaux, en partage comme en discussion.* » (Farge, 2002). Ainsi la portée d'un évènement se mesure à l'impact qu'il a tant sur le plan physique que sur le plan du discours, que ce dernier soit relayé par les médias ou pas.

Le philosophe Paul Ricœur définit l'évènement comme toute occurrence physique, et celui-ci devient historique sous trois conditions : « *produit ou subi par des humains, […] jugé suffisamment intéressant ou important par les contemporains pour que les rapports qu'en font des témoins oculaires crédibles soient enregistrés. […] la mise en intrigue, qui introduit un premier décalage épistémique entre l'évènement tel qu'il est survenu et l'évènement tel qu'il est raconté, enregistré, communiqué.* » (Ricœur, 1992). Cette définition apporte un nouvel éclairage à la notion d'évènement. Puisque celui-ci doit être raconté, il y a une faille d'analyse possible entre le vécu, le perçu et le compris.

La prise en compte de l'évènement par les historiens dépend de l'école à laquelle ils sont affiliés. Chez les historiens français de l'École des Annales, à l'Histoire des dates succède, la Nouvelle Histoire, puis l'Histoire des mentalités, qui se voit relayée par l'Histoire des représentations. Ce mouvement générationnel tend à replacer l'individu, l'évènement individuel dans l'Histoire. Selon l'historien Pierre Nora : « *les mass médias ont désormais le monopole de l'Histoire* ». Il précise même : « *pour qu'il y ait évènement, il faut qu'il soit connu* », tout en reconnaissant que les mass médias ne peuvent que « *favoriser l'éclosion d'évènements massifs* ». En définissant l'Histoire contemporaine, composée d'évènements modernes, Nora prend une analogie militaire qui n'est pas sans rappeler le concept de guerre hybride que nous

aborderons ultérieurement : « *Cette histoire attend son Clausewitz pour analyser la stratégie de l'événement total qui, comme la guerre, a enrôlé les civils ; il n'y a plus d'arrières de l'histoire, pas plus que de front unique où combattraient les militaires.* » (Nora, 1972).

On comprend ici, que du nombre infini de faits qui se produisent quotidiennement, certains deviennent des évènements historiques à cause de leur impact et le discours sur l'évènement ainsi que les médias par lequel l'évènement est connu auront un impact sur la qualification du fait comme évènement. Il apparaît donc nécessaire d'être en mesure d'identifier lesquels, parmi les faits, constituent une rupture. Ceci nous permet d'introduire une autre définition de l'*évènement* en tant que fait de rupture, une définition issue du renseignement militaire. Les évènements relèvent ainsi d'anomalies dans le cours quotidien des faits, plus particulièrement d'anomalies pouvant avoir valeur d'indices d'alertes (APAVIA) concept qui entre notamment dans le cadre du renseignement d'alerte, c'est-à-dire : « *une forme de renseignement de situation qui se focalise sur un changement significatif de celle-ci.* » (CICDE, 2010 a). Le renseignement militaire doit donc être en mesure de détecter les évènements.

Pour le militaire français, le processus de création de renseignements est défini comme étant une information validée, ou une évaluation tirée d'informations validées. Cette définition place l'analyse de l'information au cœur de ce dispositif d'appui à la décision. Derrière la notion d'analyse de l'information se cachent à la fois un processus de traitement c'est-à-dire la capacité à extraire les informations des données et un processus d'exploitation c'est-à-dire le regroupement, la cotation, l'analyse, la fusion et l'interprétation des informations en vue de fournir une réponse à une question. Cette approche structurée est particulièrement adaptée pour le traitement de données issues de systèmes conçus pour et par les forces armées, en particulier lorsque ceux-ci sont orientés pour exploiter des informations en provenance de capteurs conçus à cette fin. La question se pose de savoir si elle adaptée aux mass média, ou aux médias sociaux. Or, ces derniers vecteurs sont ceux les plus à même de capter les évènements.

Si l'internet est entré progressivement dans la sphère informationnelle des services de renseignement au titre de renseignement de sources ouvertes, les méthodes de traitement et d'exploitation des informations permettent-elles d'utiliser au mieux l'information diffusée par cette évolution qu'est le réseau social numérique ? Il est permis d'en douter à plusieurs titres. Une première raison vient du fait que le média social numérique est relativement récent, les plus utilisés aujourd'hui n'existaient pas avant 2006 et aucun n'a atteint une taille suffisamment critique avant 2009 pour compter significativement dans la masse d'information disponible sur un sujet donné susceptible d'intéresser un service de renseignement. Internet évoluant à un

rythme beaucoup plus élevé que la doctrine militaire, il est probable que les méthodes d'analyse aient besoin d'être adaptées. De plus, la recherche en Sciences Humaines et Sociales notamment en Sciences de l'Information et de la Communication est encore en train de poser les bases conceptuelles du/des rôle(s) du réseau social numérique dans la société. Quant au renseignement militaire, le rôle du média social dans le système sociétal d'une nation en période de conflit est sujet à discussions. En effet que peut-on apprendre des émetteurs du réseau et quels renseignements peut-on en tirer ?

La recherche présentée ici sur la détection d'évènements au service du renseignement de sources ouvertes souhaite contribuer à deux domaines : celui des sciences de l'information et de la communication et celui de la pensée militaire. Il s'agit de montrer comment les méthodes d'exploitation des mégadonnées (« big data ») issus du contenu généré par les utilisateurs sur les réseaux sociaux permettent de détecter les événements en cours et d'en apprécier l'importance ainsi que leurs conséquences possibles (partie II). Par là même nous montrons que la notion d'*évènement* dont la conception traditionnelle en communication la définit par rapport aux médias de masse (presse, radio et télévision) doit être repensée car elle est aujourd'hui construite au sein des échanges entre de multiples acteurs par l'intermédiaire des réseaux sociaux. Des recherches en sciences de l'information sur ce qui est souvent nommé « event tracking » ou « event detection » commencent à se développer (voir par exemple Seifickar et Farzi, 2019). Ces recherches concernent de multiples types d'évènements, souvent des désastres naturels ou des phénomènes de communication de crise. La particularité de cette thèse est d'aborder les conflits politiques caractéristiques des guerres modernes. Les acteurs construisant l'événement sur les réseaux sociaux peuvent être des médias, mais sont aussi des témoins et diverses forces tentant d'influencer le terrain en situation de conflit. La méthodologie du renseignement militaire de sources ouvertes, très dépendante de celle des médias de masse, s'en trouve affectée (partie I) tout comme la conception de l'information dans les guerres modernes, dites « guerres hybrides » (partie I). En mettant en évidence la place de l'information dans ces conflits, nous en tirons les conclusions relatives à de nouvelles dimensions de la « maîtrise de l'information » (partie III), concept commun aux sciences de l'information et à la pensée militaire.

L'objet et le terrain de cette recherche sont ancrés dans notre parcours professionnel. Engagé dans la Marine Nationale en 1996, nous réussissons en juin 2003 les épreuves de sélection de l'école interarmées du renseignement et des études linguistiques (EIREL) pour y suivre un cursus de renseignement et de langue russe. Ce diplôme d'opérateur linguiste d'interception en

langue russe entre dans le domaine du renseignement d'intérêt militaire. L'interception consiste à écouter des réseaux de télétransmission, trier les informations et rendre compte rapidement de tout événement important. La traduction consiste à traduire en langue française le produit de l'interception et d'en faire une première analyse avant exploitation au niveau fonctionnel supérieur. Entre 2005 et 2007, nous avons consacré deux années à la mise en place de la chaîne de recueil de renseignements sur internet du centre de renseignement de la marine nationale. De 2007 à 2009, nous avons dirigé l'exploitation de cette chaîne de recueil et notamment participé à la rédaction d'un nouveau niveau de formation au profit du personnel dédié à cette branche. Tout en occupant les fonctions précitées, nous avons pu également prendre part au développement d'un concept interarmées du recueil de renseignements sur internet. En juillet 2009, nous avons été sélectionné pour devenir l'assistant de l'attaché de défense près les ambassades de France en Ukraine et Biélorussie. Cette mission de trois années nous a permis d'exploiter au quotidien mon expertise dans le recueil et d'analyse pour dresser une situation actualisée de ces deux pays aux frontières de l'Europe. A notre retour en 2012, nous avons été affectés à la direction du renseignement militaire jusqu'à ce que la crise ukrainienne éclate. Nous avons alors mené notre dernière mission au service du Ministère de la Défense avec un déploiement de plusieurs mois au cœur du conflit. Cette expérience professionnelle nous a amené tout au long de notre carrière à nous interroger sur les difficultés à détecter les évènements et à exploiter les données de masse, en particulier issues d'internet et des médias sociaux.

La première partie de nos travaux porte sur le cadrage théorique et contextuel de notre recherche, à savoir pourquoi détecter les évènements plutôt que chercher à prédire les comportements dans le contexte du renseignement de sources ouvertes en situation de conflit.

Le chapitre 1 portera sur l'intelligence artificielle au service du renseignement de sources ouvertes. Il s'agira dans ce chapitre d'effectuer un état de l'art de la prédiction de comportement, vœu pieu du béhaviorisme appliqué tant dans le domaine du marketing que du terrorisme. Nous inscrirons ce chapitre plus particulièrement dans les situations de conflit ; nous nous appuierons donc sur les sciences humaines et sociales, plus particulièrement sur l'étude des mouvements sociaux et reprendrons les principes et pratiques du « protest event analysis » (PEA) pour évaluer leurs contributions à la détection d'évènement. Enfin, nous poursuivrons l'étude de la détection et de l'analyse des évènements dans le contexte des nouvelles

technologies de l'information et de la communication (NTIC) en illustrant notamment les rôles de l'exploitation analytique des données et de l'intelligence artificielle.

Le chapitre 2 portera sur la nécessaire évolution du cycle du renseignement. Après avoir revu les principes et pratiques du renseignement, nous l'inscrirons dans le contexte de la guerre de l'information. Cette dernière rend nécessaire le fait de repenser l'analyse des données pour le renseignement d'origine sources ouvertes.

Dans le chapitre 3, nous poserons les principes définissant un théâtre d'opérations connecté. Nous observerons le cycle de vie de l'information sur les réseaux sociaux avant d'étudier les pratiques des sciences sociales computationnelles pour analyser ces informations.

La deuxième partie de notre recherche illustrera notre méthodologie de détection d'évènement à un terrain d'observation : la crise ukrainienne de novembre 2013 à juin 2014. Ce conflit réunit de nombreuses caractéristiques d'affrontements en cours et à venir notamment par le volume d'informations disponibles sur les médias sociaux pendant toute sa durée.

Nous commencerons cette partie, dans le chapitre 4, par un état de l'art des algorithmes de détection. Nous enchaînerons avec la description de notre méthodologie Deteven et expliquerons comment l'approche par la notion de lieu (la toponymie) permet une bonne détection d'évènement. En effet, l'évènement est doublement ancré dans le concept de lieu car le discours positionne tant l'évènement que le locuteur en un seul et même endroit ou en deux lieux séparés. Enfin nous décrirons la pertinence de cette approche sur un média social en particulier : Twitter.

Dans le chapitre 5, nous décrirons la mise en œuvre de la plateforme Deteven dans les contextes du conflit ukrainien. Nous commencerons par une chronologie des évènements, que nous inscrirons ensuite dans le contexte spécifique de la guerre hybride et des médias sociaux en Ukraine avant d'expliquer comment suivre une révolution sur Twitter au moyen de la plateforme Deteven.

Dans le chapitre 6, nous porterons notre attention sur les biais de méthodologie et de l'intelligence artificielle. Plus particulièrement nous regarderons les outils d'analyse statistique, sémantique et relationnelle ainsi que la collecte de données sur médias sociaux pour en expliquer les contraintes.

La troisième et dernière partie de notre recherche inscrira nos travaux de détection d'évènement dans le contexte de la maîtrise de l'information. Cette maîtrise à pour but de rendre l'individu, le citoyen, la société dans son ensemble plus résilients face aux menaces décrites précédemment.

Dans le chapitre 7, nous illustrerons nos travaux par deux applications concrètes. Tout d'abord nous donnerons un exemple de système de suivi de l'influence étrangère en période électoral. Nous analyserons ensuite le parcours d'une fake news, de sa création à sa diffusion.

Dans le chapitre 8, nous appliquerons la méthodologie de la partie II aux forces de l'ordre. Si le renseignement guide l'action des armées, il peut tout autant guider les forces de police sur le territoire national. Cependant, il faut bien distinguer les fantasmes de la police prédictives de la réalité de la police guidée par le renseignement (Intelligence-led policing).

Le chapitre 9 développera le concept de maîtrise de l'information de la sécurité individuelle à la sécurité collective. Si nous confions notre sécurité aux forces armées et aux forces de l'ordre, il est également nécessaire à chaque individu de maîtrise son environnement informationnel, comme à chaque société de fournir à ses citoyens une éducation aux médias et à l'information. Enfin cette maîtrise ne serait rien si l'on n'est pas en mesure de maintenir un internet de confiance, neutre, et gouverné dans l'intérêt commun.

Première partie : Le renseignement d'origine sources ouvertes en situation de conflit : détecter plutôt que prédire

Introduction de la première partie

En France, la fonction renseignement n'a jamais été une fonction noble des forces armées à l'opposé de la pensée anglo-saxonne qui la tient en haute estime. De plus, parmi les types de renseignement, le renseignement de sources ouvertes (ROSO) est très souvent dénigré. Considéré également comme non noble, voire peu fiable, il ne bénéficie pas, loin s'en faut, du même investissement cognitif et financier que les autres types de renseignement tels que le renseignement humain, le renseignement d'origine image ou le renseignement d'origine électromagnétique.

La fonction renseignement n'est arrivée que tardivement sous le feu des projecteurs en 2013 comme fonction stratégique « anticipation et connaissance ». Cette reconnaissance coïncide avec plusieurs changements stratégiques ou plutôt « surprises stratégiques » tels que les printemps arabes ou l'apparition d'un mouvement djihadistes en bande sahélo-saharienne. S'il y a bien un domaine dans lequel le renseignement de sources ouvertes apporte un point de vue à nul autre pareil, c'est l'observation et l'analyse des mouvements sociaux, d'autant plus quand ces derniers s'expriment en ligne sur les réseaux sociaux. Cette capacité est primordiale car lorsqu'ils ont lieu dans des États fragilisés, ces mouvements peuvent dégénérer en guerre civile voire en guerre tout court.

Le premier chapitre abordera la nécessaire évolution du renseignement de sources ouvertes. En premier lieu, pour être en mesure d'anticiper les évolutions des mouvements sociaux, il faut en comprendre les dynamiques et donc intégrer les travaux réalisés en sciences humaines et

sociales sur les théories du conflit. Nous aborderons une méthodologie en particulier, le « protest event analysis », que nous adapterons au besoin du renseignement et aux capacités de l'intelligence artificielle. Enfin nous expliquerons qu'anticiper n'est pas prédire, le terrain ne s'y prête pas. Il est par contre essentiel d'être en mesure de détecter les évènements qui s'y passent.

Le second chapitre portera sur la nécessaire évolution du cycle de renseignement. Nous verrons tout d'abord les principes et pratiques du renseignement tel qu'il est fait actuellement. Puis nous décrirons le contexte de guerre de l'information dans lequel le ROSO se pratique. Enfin nous proposerons une méthodologie pour pouvoir intégrer de nouvelles données, des méga-données issues de l'internet, en utilisant les mêmes technologies que le Web qui les diffusent.

Dans le troisième et dernier chapitre de cette première partie de nos travaux, nous inscrirons le ROSO dans un contexte qui dépasse le strict champ de bataille militaire. La guerre hybride conceptualisée comme un état permanent d'affrontement entre les nations est particulièrement visible sur les médias sociaux. Cette guerre s'exprime dans un nouveau genre de théâtre d'opérations, le théâtre connecté. Nous en décrirons les évolutions de 2009 à 2014. Enfin nous nous intéresserons aux processus de création, de diffusion, et d'influence sur les réseaux sociaux.

1. Chapitre 1 : Évolution du Renseignement de sources ouvertes sur les terrains de conflit : enjeu et méthode à l'âge du Web.

1.1. Introduction

Ce chapitre présente la modélisation possible d'un conflit politique pour l'exploitation en machine des informations nécessaires au renseignement de sources ouvertes (ROSO). Un des domaines où le ROSO surpasse d'autres capteurs est celui du renseignement de situation qui requiert une connaissance du terrain humain dans lequel va s'inscrire l'opération militaire. Or ce terrain humain s'exprime sur les réseaux sociaux. Nous commencerons par illustrer les intérêts communs et donc la logique liant le ROSO, les SIC et les SHS au travers des théories du mouvement social. Chaque étape de la construction d'un mouvement social, chaque mécanisme mis en œuvre sont autant d'indicateurs d'évolution dudit mouvement qu'il est possible de recueillir par les réseaux sociaux et de traiter ensuite au travers d'une plateforme d'exploitation analytique.

Ce chapitre montrera l'intérêt, mais aussi les limites du « protest event analysis » (PEA) et la pertinence de la théorie du sociologue Tilly. Il en tire les conséquences d' une approche du renseignement centrée sur les événements et non essentiellement sur les individus puis expose comment cette approche peut être rendue opérationnelle alors que le développement de l'intelligence artificielle et des données massives donnent au renseignement ouvert des moyens nouveaux.

1.2. L'apport de la théorie du conflit au ROSO

Lors de la 14ème université d'été de la Défense en 2016, Manuel Valls, 1er ministre français, disait : « *Nous faisons face – c'est la donnée essentielle – à une mutation profonde de l'équation de sécurité, avec un continuum inédit, mais majeur, entre sécurité intérieure et sécurité extérieure, entre les problématiques de sécurité et de défense* » (Valls, 2016). Cette recherche s'inscrit dans un continuum identique à celui décrit par Charles Tilly qui établit une continuité dans les politiques du conflit de la manifestation à l'émeute, du mouvement social à la révolution, de la guerre civile à l'intervention extérieure, un pan nouveau de la recherche en se situant à la frontière des actions collectives et des conflits armés, frontière rarement franchie par les sociologues de la contestation : "*nos idées sur la Dynamique [du conflit] ne s'avançaient pas aussi loin que celles de Tilly : il voulait inclure la guerre - la forme la plus extrême de contestation - dans notre répertoire de contestation.*" (Tilly et Tarrow, 2015). La fonction renseignement dans le contexte de ce continuum ne peut se passer de l'information diffusée sur l'internet par les parties prenantes des mouvements sociaux.

La généralisation de l'usage d'internet offre un nouveau moyen d'action collective permettant, grâce aux médias sociaux, la mise en réseau des intelligences, la mise en commun des moyens de financement, la mutualisation des moyens de l'action militante. Sans cet ancrage dans les sciences humaines et sociales (SHS) et plus particulièrement dans la politique du conflit, cette recherche aurait été limitée à la modélisation de situations insurrectionnelles ou de quasi-guerre. Les SHS ont permis de modéliser, plus en amont encore, l'image que reflètent les réseaux sociaux d'un conflit et ce dès les premières manifestations et émeutes. Le résultat de ces efforts de recherche permettrait aux services pratiquant le ROSO s'ils étaient pris en compte de mieux exploiter les informations recueillies, notamment en établissant des indicateurs d'alerte.

« *Pratiquement tous les plaisirs que l'homme tire de la vie sociale se retrouvent dans les mouvements de contestation : sens de la communauté et de l'identité ; compagnonnage et liens continus avec d'autres ; la variété et le défi de la conversation, de la coopération et de la compétition. Certains des plaisirs ne sont pas disponibles dans les routines de la vie.* » (Jasper, 1997). On pourrait facilement remplacer « mouvement de contestation » par médias sociaux et la citation garderait tout son sens.

Le terme « *mouvement social* » est souvent utilisé pour décrire un large éventail de transformations sociales dans un certain nombre de domaines, conduisant à la prolifération de

définitions et de descriptions. Parmi les définitions des mouvements sociaux, les premières théories mettent en évidence le caractère non institutionnalisé et organisé au minimum des actions collectives qui se structurent autour de griefs spécifiques (mécontentement) afin de promouvoir - ou de résister au changement social (Wilkinson 1971 ; Tilly, 1978 ; Jenkins, 1983). Ces théories fondamentales issues des travaux en sociologie de Durkheim posent l'action collective comme une rupture de l'équilibre social. Parmi les approches les plus populaires on trouve en ordre chronologique le conflit de classe (1880), l'action collective (1950), la théorie de la valeur ajoutée (1960), la théorie de la mobilisation des ressources (1970), la théorie des cadres et la théorie du processus politique (1980).

Ces différentes perspectives peuvent être attribuées à des conceptions théoriques changeantes, voire opposées parmi les universitaires, mais ont également émergé à travers l'analyse de nouvelles formes de mobilisation sociale à travers les décennies.

Aujourd'hui, chaque théorie peut bénéficier des apports des nouvelles technologies de l'information dont notamment les réseaux sociaux numériques.

La théorie de la mobilisation des ressources découle de l'analyse des mouvements des années 1960. Elle souligne l'importance des ressources dans la promotion du changement social (Jenkins, 1983; Jenkins et Perrow, 1977; McAdam et al., 1997). La formation et la mobilisation de mouvements dépendent des changements de ressources, d'organisation du groupe et d'opportunités d'action (Jenkins, 1983). Les mouvements sont également évalués en fonction de leur capacité à rassembler et à utiliser des ressources pour apporter des changements. Les ressources sont considérées comme des actifs matériels ou immatériels apportés par des groupes et des individus au sein du mouvement et jouent un rôle important dans la capacité du mouvement à atteindre son objectif (Freeman, 1978; Horn, 2013). Parmi les ressources à acquérir, l'importance de la communication est déjà soulignée en 1977 par McCarthy et Zald : « *Des médias libres sont probablement nécessaires pour impliquer en masse les constituants isolés dans les flux de ressources, par conséquent, les adhérents isolés contrôlant de vastes réserves de ressources sont probablement plus importants pour la croissance des industries de mouvements sociaux dans les sociétés sans médias de masse.* » (McCarthy, Zald, 1977).

Les réseaux sociaux numériques contribuent activement à compenser l'absence de contrôle sur d'autres médias de masse lors des situations de conflits même si leur portée est discutée. « *la relation entre les divers types médias sociaux numériques et l'activisme numérique est complexe et dépend fortement du contexte politique et national.* » (Breuer, 2011). Certains chercheurs limitent les contextes favorables à la contribution active des médias sociaux : « *les médias*

sociaux facilitent la mobilisation politique, mais uniquement dans les pays non démocratiques. » (Bridwell, 2013).

Les réseaux sociaux numériques permettent de contribuer au capital à mobiliser dans un mouvement social :

- Moral : expression de la solidarité, légitimité et le soutien de sympathisant. La diffusion de ces messages sur les réseaux sociaux est observée dans la plupart des conflits.
- Culturel : comment accomplir des tâches spécifiques comme organiser un évènement de protestation, tenir une conférence de presse, organiser une réunion, constituer une organisation, initier un festival ou diffuser sur le Web. Ce savoir est disponible sur de nombreuses ressources en ligne, notamment probablement la plus importante comment communiquer de façon chiffrée, comme le propose par exemple Reporter Sans Frontières avec son kit de sécurité numérique. (RSF, 2016).
- Socio-organisationnel : la distribution de tracts, l'organisation de réunions communautaires, le recrutement de volontaires. L'ensemble de ces messages est régulièrement diffusé sur les réseaux sociaux.
- Matériel : capital financier et physique, comme les bureaux, l'argent, l'équipement et les fournitures. Par exemple en Azerbaïdjan, après la mise en place de contraventions pour participation à une manifestation des appels aux dons ont été lancés sur Facebook récoltant plus de 13 000 dollars en une semaine (Pearce, 2014a).
- Humain : ressources telles que le travail, l'expérience, les compétences et l'expertise dans un certain domaine. Par exemple l'appel à toute personne du corps médical à participer aux infirmeries de campagne après les affrontements les plus violents avec les forces de l'ordre à Kiev.

« *Bien que certains chercheurs pensent que la théorie de la mobilisation des ressources a atteint son apogée et que, même si la recherche sur l'utilité des médias sociaux dans les mouvements sociaux en est encore à ses balbutiements, leur combinaison tirerait parti de l'endurance et de la force de la théorie tout en la réactualisant pour l'époque contemporaine.* » (Eltantawy, Wiest, 2011).

La théorie des cadres utilise une approche centrée sur la psychologie cognitive, la linguistique et l'analyse des discours, les études de communication et des médias pour définir le rôle des idées dans la construction d'un mouvement social. Elle critique la théorie de la mobilisation de ressources en lui reprochant une approche centrée sur l'organisation structurelle et politique

sans prendre en compte la construction sociale. Dans cette approche, le cadrage est le processus actif de construction d'interprétations, de représentations et de significations partagées de situations et de problèmes sociaux (Snow & Benford, 1988). Cette théorie a été particulièrement étudiée et appliquée sur les mouvements des années 90 au point où : « *De toute évidence, on assiste à une prolifération prononcée des travaux d'information sur les cadres d'action et les processus d'encadrement en relation avec les mouvements sociaux au cours des quinze dernières années, à tel point que les processus de cadrage été considérés, parallèlement à la mobilisation des ressources et aux processus d'opportunité politiques , comme étant une dynamique centrale dans la compréhension du caractère et du cours des mouvements sociaux.* » (Benford & Snow, 2000).

La conversion de ce concept de la psychologie à la sociologie a été faite par Goffman (1974) qui s'intéressait à l'enchainement : création d'un discours, diffusion d'une culture et comment ces éléments influent et contraignent les interactions entre individus. Ainsi une tendance forte identifiée dans les mouvements sociaux est l'alignement des cadres (framing alignment) c'est-à-dire la tendance vers une convergence des idées individuelles dans un creuset commun pour une cause commune. Comme tous les participants ont des cadres différents, il est nécessaire d' « aligner » les cadres individuels pour que les intérêts, les croyances et les valeurs de chacun soient en harmonie avec les activités, les idées et les objectifs du mouvement (Snow, et al., 1986). Les cadres de l'action collective sont construits par la négociation entre les adhérents du mouvement afin d'identifier une condition ou une situation qui, selon eux, nécessite un changement, de formuler une solution et de motiver les autres à agir (Benford et Snow, Op.cit.). Les processus d'encadrement soulignent l'importance de donner un sens et impliquent la redéfinition de phénomènes sociaux incontestés, produisant des compréhensions alternatives de situations prises pour acquises (Lehrner & Allen, 2008; Maton, 2008).

Ces processus mènent à la définition d'une cause commune, d'une vision centrale qui guide l'action et fédère les membres (Horn, Op.cit.). Cet alignement se réalise sous quatre formes :

- Frame bridging (aligner plusieurs cadres s'accordant, mais non liés)
- Frame amplification (clarification et amplification)
- Frame extensions (atteindre de nouveaux soutiens)
- Frame transformation (redéfinir et recentrer le cadre primaire)

Chacune de ces formes a été observée par Linda Hon dans ses travaux portant sur le mouvement « Million Hoodies » étudié à partir de ses posts sur le média social Facebook ; (Hon, 2016). Le

relais médiatique exceptionnel que représente les médias sociaux sert de caisse de résonnance à l'ensemble des efforts de définition et d'adaptation des cadres d'un mouvement social.

Le concept de théorie du processus politique souligne l'importance des contextes politiques et des opportunités pour l'émergence et le développement de mouvements sociaux (Goodwin et al., 1999; Horn, Op.cit.; McAdam et Snow., 1997). Les mouvements sociaux se développeraient de manière dynamique en réponse à des opportunités contingentes (considérées comme des changements structurels politiques et des changements de pouvoir) qui influencent leurs efforts pour mobiliser leurs membres et leurs ressources (Goodwin et al., Op.cit.; Meyer et Minkoff, 2004). Dans cette perspective, certains contextes sont plus propices aux activités de mouvement social et à la valorisation des opportunités politiques (Meyer et Minkoff, op. cit..).

Ces opportunités peuvent inclure l'instabilité politique résultant d'un conflit entre les élites ou à un processus de prise de décision politique ou tout autre évènement ayant les attributs caractéristiques d'une injustice aux yeux d'une partie de la population. Bien que le cycle de vie d'un mouvement social soit défini différemment en fonction de l'approche théorique particulière utilisée, quatre grandes étapes sont identifiées.

La première étape est la phase d'émergence, qui représente la construction de l'infrastructure du mouvement (par exemple, une large base de membres activistes, des réseaux, des centres d'organisation) en réponse à un mécontentement général face à un problème.

Dans un deuxième temps, l'identité et la vision du mouvement se développent autour d'un discours interprétatif clair, le mouvement devenant plus organisé et stratégique.

La troisième étape est une étape de transformation à travers laquelle le mouvement met en œuvre son action collective. Déclinaison spécifique d'action collective d'un mouvement social, le conflit social s'inscrit dans le champ d'études des politiques du conflit (contentious politics). Durant cette quatrième phase, le mouvement bénéficie du pouvoir politique et d'un fort niveau d'organisation pour progresser vers son objectif.

D'après Charles Tilly, les attributs de cette phase sont : les démonstrations publiques de longue durée qui expriment l'objet de la contestation ; la réclamation exprimée ; les répertoires de contention c'est-à-dire un ensemble de stratégies et de tactiques disponibles à groupe spécifique dans contexte spatiotemporel déterminé ; enfin les expressions de la valeur, de l'unité, du nombre et de la détermination. Ce dernier attribut rassemblé sous l'acronyme WUNC (worthiness, unity, number, commitment) correspond en grande partie à la raison pour laquelle une personne utilisera un réseau social numérique. Ces outils sont massivement utilisés au quotidien, s'invitent dans tous les aspects de la vie en société et donc *a fortiori* dans les

mouvements de contestation. Ainsi notre recherche s'inscrit dans le cadre général de l'étude des mouvements sociaux, plus particulièrement dans l'étude des répertoires d'action collective tels que définis par Charles Tilly (Tilly, 1984). Ces répertoires sont donc des inventaires des modes d'expression de la contestation populaire. La nature même des conflits entre prévisibilité potentielle et « *moments de folie* » (Zolberg, 1972) appelle une approche interdisciplinaire pour tirer des conclusions allant au-delà des contraintes techniques, des préjugés personnels et de l'interprétation subjective de l'ensemble de données. Une fois encore pour que le renseignement puisse tirer toute la connaissance possible des moments de conflits il doit intégrer des savoirs maîtrisés par les SHS. Les trois fonctions clefs ci-après, basées sur les travaux de la Dynamique de la contestation (McAdam et al., 2001) bénéficient toutes d'une utilisation des médias sociaux : constitution de nouveaux acteurs politiques et d'identités pendant les épisodes de contestation, polarisation de certain groupes politiques, changement d'échelle dans la contestation politique, de l'arène locale à l'arène trans-locale (voire transnationale).

La constitution de nouveaux acteurs est renforcée puisque tout utilisateur des médias sociaux est un créateur/diffuseur d'information. Chacun a, intrinsèquement, l'opportunité d'être acteur de la contestation. Avec l'avènement de l'appareil photo intégré au téléphone connecté à l'internet, toute personne peut témoigner d'injustice, exprimer son opinion, appeler sa base d'amis numériques à relayer son message lui permettant ainsi de mesurer son influence en temps réel.

La polarisation est plus facile à augmenter. Les médias sociaux permettent à des informations de circuler massivement au sein d'une communauté. Le principe de viralité, le buzz, est un constat : une information polarisante génère des fédérations et des sécessions, des regroupements de partisans d'un côté du débat et d'opposants de l'autre ajoutant à la surenchère.

Le changement d'échelle est accéléré. Avant les médias sociaux, les crises pouvaient être largement contenues localement grâce au contrôle quasi absolu des régimes autoritaires sur les médias. Seuls des envoyés spéciaux étrangers, la diaspora, les dissidents exilés étaient à même de communiquer sur une situation de conflit local. Aujourd'hui, les médias sociaux donnent accès à une audience mondiale à n'importe quel utilisateur.

D'autres fonctions subsidiaires sont renforcées telles que :

- Mobilisation : incitation à participer dans le but d'atteindre une masse critique auto-mobilisatrice (Barnes, et Böhringer., 2009).
- Cadrage de la contestation : ce qu'on revendique et pourquoi on le revendique.

Enfin, au moment des évènements sur le terrain, des fonctions opérationnelles, voire militaires, sont mises en œuvre parmi lesquelles l'image opérationnelle commune (Starbird, et al., 2010), la communication et la coordination d'activités.

En effet l'approche théorique portant sur l'identification des mécanismes et processus sous-jacents d'une action collective d'envergure apporterait de nouvelles grilles d'analyses, de nouveaux indicateurs au renseignement sur, par exemple, la polarisation de parties prenantes, la radicalisation d'acteurs, l'identification de personnes d'intérêt.

Ces mécanismes et processus semblent pouvoir donner lieu à des modélisations permettant d'en détecter automatiquement l'émergence. Ainsi, la transformation d'une théorie en un ensemble de processus/évènements reconnaissables automatiquement jusque-là non employés dans les systèmes d'analyse du renseignement nous paraît nécessaire. C'est l'enjeu de cette thèse.

À titre d'illustration, ci-dessous quelques mécanismes théorisés qu'il semble possible de modéliser donc d'en identifier des caractéristiques statistiques, sémantiques et relationnelles :

- Certification : reconnaissance des protagonistes par des autorités extérieures. Détecter le moment à partir duquel un nouvel acteur politique devient identifiable puis identifié par d'autres acteurs nationaux ou internationaux.
- Émulation : imitation consciente d'une représentation observée ailleurs. Identifier le processus de circulation de l'information pouvant entraîner cette émulation, estimer les probabilités de recréation d'une forme de contestation en fonction de la diffusion de l'information et de l'analyse du ressenti des récepteurs de cette information.
- Intermédiation : production d'une liaison entre deux sites jusque-là disjoints ou faiblement connectés. Caractériser les éléments techniques permettant de prouver un partage d'idées ou de moyens entre deux sites.
- Appropriation sociale : transformation d'une organisation en entité politique. Reconnaître les marqueurs types d'une entité politique dans un contexte local, mode de diffusion de l'information, capacités de mobilisation, thématiques choisies, positionnement.
- Changement d'échelle : augmentation/diminution du nombre d'acteurs ou de la portée géographique d'une revendication coordonnée. Identifier quels paramètres, autres que statistiques permettraient de prouver un changement d'échelle.

- Changement d'identité : nouvelles réponses aux questions : Qui sommes-nous? Qui sont-ils? Qui êtes-vous? Suivre les valeurs, images, idées, partagées au sein d'une communauté et alerter sur leurs évolutions.
- Involution : évolution d'organisation dans le sens de la fourniture de services sociaux à leurs membres. Il s'agit d'une manœuvre souvent observée dans les phases initiales d'un conflit ou au moment d'une conquête de territoire, un acteur décidant d'affronter un État en remplace les services par les siens (Frères Musulmans en Egypte, Daesh en Syrie, Nouvelle Russie en Ukraine). Ce phénomène devrait pouvoir être détecté par une analyse automatisée.
- Mobilisation / Démobilisation : évolution des ressources à disposition d'un acteur pour sa revendication. Identifier l'évolution de l'accès à ces ressources matérielles telles que l'argent, les installations et les moyens de communication et les ressources humaines intangibles telles que l'organisation des compétences et le travail des supporteurs.
- Polarisation : accroissement de l'écart idéologique entre différents acteurs, par exemple identifier l'évolution du sentiment franchement pour ou contre un concept.
- Radicalisation : évolution vers un profilage plus marqué des acteurs, identifier automatiquement les enchaînements logiques préalablement caractérisés.

Parmi les pistes à explorer pour atteindre un niveau de maîtrise suffisant des données de masse, le lien entre le monde militaire et le monde académique est bien mis en évidence dans les conclusions des travaux d'une mission d'information sur les enjeux de la numérisation des armées écrite par les députés Becht et Gassilloud : « *la recherche civile (académique ou appliquée) peut être indirectement à l'origine de services et dispositifs duaux utiles à la défense nationale, citant les domaines suivants :[] l'intelligence artificielle et la « fouille de données » (data mining), notamment en lien avec des recherches en sciences humaines et sociales sur les comportements humains.* » (Becht, Gassiloud, 2018). Force est de constater que tant les budgets que le nombre de projets conjoints en France sont bien en dessous de ce qui se fait dans d'autres nations, alors qu'il est évident que l'interaction entre renseignement et université est bénéfique et a été démontrée à de maintes reprises et depuis un certain temps déjà. (Irondelle et Malissard, 2011).

Les théories du conflit issues sont un outil indispensable pour la fonction renseignement. Elles permettent de comprendre un mouvement social et d'en maîtriser les dynamiques.

1.3. Le Protest Event Analysis et l'intelligence artificielle

À la fois cadre théorique et boîte à outils employée pour étudier le mouvement social, une méthodologie s'illustre depuis les années 80/90 : le protest event analysis (PEA) : « *En effet, et en tout premier lieu, en offrant de penser la relation diachronique entre développement des mouvements et contextes, la PEA a permis de nets profits de connaissance en matière d'identification et d'analyse des modalités de fonctionnement des répertoires, des cycles de mobilisation et des effets de la répression* » . (Fillieule, 2007). Cette méthodologie regroupe à la fois une approche quantitative et qualitative basée sur une analyse de contenus pour la plupart issus de la presse écrite. Elle s'appuie sur une analyse chronologique des évènements contestataires dans un environnement donné. L'objectif est de regrouper l'intégralité des articles de presse portant sur un évènement (approche quantitative) et d'en exploiter le contenu au travers de séries temporelles (approche qualitative).

Pour Hutter, le PEA :

- est un type d'analyse de contenus (quantitative),
- transforme les mots en chiffres,
- permet la cartographie des occurrences et des caractéristiques de manifestations au travers des zones géographiques, des problématiques/mouvements et au travers du temps,
- est étroitement lié à l'approche du processus politique.

Il analyse quatre générations de PEA. La première met en place la méthodologie, la seconde renforce la rigueur de l'encodage, la troisième prend mieux en compte les biais des sources et la quatrième étend l'encodage pour intégrer un plus large éventail d'indicateur d'évènements (Hutter, 2014). Qu'il s'agisse de l'étude des manifestations pour les droits civiques aux États-Unis (McAdam, 1999), ou sur les cycles de contention en Italie de 1965 à 1974 (Tarrow, 1989) ou les nouveaux mouvements sociaux à travers l'Europe occidentale (Kriesi et al., 1995) le PEA est la méthode de référence dans l'analyse des mouvements sociaux.

Cette méthodologie attire plusieurs critiques. La première porte sur la sélection de la source : « *Toutefois, il est frappant que les limites les plus nettes de cette méthode, liée au recours quasi exclusif à la presse nationale comme source, demeurent finalement éludées, malgré une abondante littérature critique.* » (Fillieule, op. cit..). En effet, le « cycle d'attention des médias

», la nature de l'évènement ou l'affiliation politique de la revue considérée sont autant de biais à une vision impartiale d'un évènement contestataire. Malgré ces critiques, dans son manuel Social Movements, The Structure of Collective Mobilization publié en 2019, Almeida estime que : « *Même en tenant compte de toutes les lacunes des journaux, ils restent, par rapport à la plupart des alternatives, la source la plus fiable, la plus durable et la plus cohérente pour étudier les manifestations sur une longue période et dans plusieurs régions géographiques.* » (Almeida, 2019).

Mis à part les médias, la principale source de PEA sont les registres de la police. Or, cette source est tout aussi biaisée, intentionnellement ou pas. En générale ni la police ni la presse ne rapporte les évènements tels qu'en aurait besoin le chercheur : « *Le problème avec les dossiers de police est que le point de vue de la police sur les évènements et la méthode pour les enregistrer ne sont pas toujours compatibles avec le point de vue des chercheurs sur le mouvement social.* » (Alexander, et al., 2016).

La seconde catégorie de critique porte sur la sélection de l'encodage et l'unité de mesure. Si la plupart des études utilisent l'apparition d'élément du répertoire de contention au sein d'une source donnée comme unité d'encodage (manifestation, sitting, émeute, etc.), il est estimé que cela ne suffit pas à dessiner le contour d'un mouvement social ou d'une contestation. De plus, l'unité de mesure est également subjective. Par exemple, si l'on décide de mesurer uniquement les manifestations de masse, il faut justifier du volume de personne correspondant. C'est la raison pour laquelle il est essentiel que le codebook comprenant l'encodage et l'unité de mesure soit mis à disposition des lecteurs (Hutter, op. cit.). Enfin, le problème de la rigueur d'encodage reste entier. Même avec un bon livre de code, le travail des encodeurs peut être source d'erreurs systématiques sur les sélection, description et encodage : il faut contrôler et échanger avec les encodeurs tout au long du projet (Semenov, 2018).

Un troisième genre de critique apparaît sur l'évolutivité de la nature de l'évènement encodé. Ainsi lorsque les acteurs d'un évènement font évoluer leur répertoire, les nouvelles expressions de la contention pourraient passer inaperçues si elles ne sont pas prévues dans l'encodage initial (Bagguley, 2010).

La quatrième nature de critique porte sur la nature des évènements suivis. Un évènement massif et avec l'État comme protagoniste est plus susceptible d'être rapporté par les médias, et la presse écrite en particulier, quand un évènement très petit et très modéré aurait tendance à être fortement sous-déclaré par les médias de masse. Par ailleurs, des biais géographiques et volumétriques apparaissent tels que : « *l'hétérogénéité spatiale, la mauvaise qualité des*

reportages dans les médias en l'absence de sources alternatives et le biais de la couverture médiatique vers les grandes villes. » (Semenov, op. cit.). Enfin, un évènement trop grand ou portant sur une trop longue durée exigerait une trop grosse collecte tant en volume qu'en durée pour être gérable (Wüest et al., 2013).

L'emploi de plus en plus fréquent de cette méthode d'analyse a permis d'apporter une plus grande rigueur dans la collecte et l'exploitation des données en SHS. Le volume de critiques qui accompagnent ces résultats a imposé une plus grande rigueur dans la description des biais des données et de leur encodage. Par exemple dans leur étude sur les PEA Filleule et Jimenez (2003) expliquent les limites à leurs travaux : faible volume de contestations collecté, sur-représentativité de certains évènements à large volumétrie ou au choix d'un mode d'action novateur. Comme le dit le sociologue Paul Bagguley : « *Nous ne devrions pas tomber dans le piège de supposer que tout ce qui est rapporté est l'intégralité de ce qui se passe. [Le PEA] Ce n'est pas l'analyse des actions des mouvements sociaux, mais l'analyse de la manière dont un débat politique public est rapporté dans les sources que nous utilisons.* » (Bagguley, op. cit.).

À suivre l'évolution des PEA, nous observons une cinquième catégorie de critique émergente, ainsi qu'une proposition pour la compenser, celle de l'étude en silos. L'approche monodisciplinaire, comme étudier un mouvement social uniquement avec des experts en sociologie ne fait plus sens aujourd'hui à l'ère du Big Data. La richesse des données, dont il est possible d'extraire une meilleure connaissance, impose de faire progresser la recherche interdisciplinaire.

Les nouvelles technologies de l'information et de communication sont de plus en plus utilisées dans les recherches portant sur les PEA. En effet : « *L'expansion rapide des techniques de Machine Learning (ML), des outils d'extraction et de récupération d'informations, ainsi que les progrès des outils de traitement du langage naturel ont ouvert de nouvelles perspectives pour l'extraction automatisée du contenu souhaité.* » (Menold et al, 2018). L'apport des NTIC permet d'adresser l'ensemble des critiques portées sur le PEA traditionnel.

Pour faire face aux critiques portant sur les biais de sources, de nombreux chercheurs se tournent vers des ressources numériques pour compenser les faiblesses du PEA traditionnel. Sur le premier volet de critiques, le choix des médias comme source, l'approche la plus recommandée reste la triangulation, c'est-à-dire le recoupement de plusieurs sources pour un évènement donné (Jenkins et Maher 2016). Non seulement les sources doivent être variées, mais également de natures différentes. Utiliser les sources en ligne permet de compenser le biais de sources de trois façons : elles fournissent des informations « non filtrées » à partir de

sites Web d'organisations mis en place par des activistes, elles comprennent non seulement des organisations formelles, mais également des organisations informelles et offrent des informations plus actualisées que d'autres sources publiques, elles facilitent l'inclusion des groupes les plus récents (Kousis et al, 2018). Cependant utiliser les médias numériques comme seule source ne suffit à compenser les biais de sélection, comme le décrivent Massimiliano Andreatta et Elena Pavan, même en utilisant un agrégateur tel que Google News, la triangulation est impossible et cette source génère de nouveaux biais. (Andretta et Pavan, 2018).

Pour compenser les biais d'encodage, plusieurs pistes sont explorées telles que l'encodage machine. Afin d'éprouver des systèmes d'encodage, il est possible de s'appuyer sur des corpus dédiés combinant : « *le codage d'évènement avec une annotation précise au niveau des symboles. Le corpus contient des évènements codés et le nombre de participants. Dans l'ensemble, nous observons un accord substantiel d'intercodeur.* » (Makarov et al, 2016). Autre axe de recherche, le programme MPEDS a pour objectif de : « *construire, tester et valider un système automatisé de codage des données de manifestation à partir de sources d'informations numérisées, en utilisant les avancées technologiques issues de l'informatique et des statistiques, à savoir le traitement du langage naturel*. » (Hanna, 2017). Le virage vers le Big Data - qui ouvre la possibilité de regarder des populations entières plutôt que des échantillons de populations (Dalton 2016) - ouvre de nouvelles perspectives sur le contexte des actions individuelles. (Lorenzini et al, 2016).

De plus en plus de chercheurs mettent en ligne des jeux de données en décrivant l'ensemble de leur méthodologie et les biais de leur jeu de données pour permettre à d'autres chercheurs de vérifier les résultats, d'inclure le jeu de données, de reprendre les méthodologies ou encore d'étalonner leurs algorithmes (Bushmann, 2018 ; Won et al, 2017 ; Lorenzini et al, op. cit.).

Le traitement des données d'évènements de mouvements sociaux utilisés dans les sciences sociales doit se faire à l'aide de méthodes importées de l'informatique et des statistiques, de la data science. Plusieurs démarches sont effectuées en ce sens telles que l'effort de collaboration entre chercheurs de la linguistique informatique et chercheurs des sciences sociales (Lorenzini et al, op. cit.).

Enfin, au-delà des critiques méthodologiques, un courant d'auteurs, notamment en France, met en évidence le fait que le PEA ne permet pas d'identifier les contextes de mobilisation et les trajectoires individuelles et appelle à : *« ne pas détacher le champ de la recherche sur les mouvements sociaux de celui sur la participation politique.* » (Fillieule, op. cit.). La capacité à

inclure une focale plus étroite, descendre au niveau local où se jouent les dynamiques d'engagement permettrait de voir des mobilisations initiales invisibles autrement (Chabanet et Royall, 2016).

La prise en compte de l'individu dans l'étude la mobilisation n'est pas antinomique à une « protest event analysis », pas plus que ne le sont une étude quantitative et une étude qualitative. Sur un sujet donné elles sont complémentaires. Dans le cas de l'étude de mouvement social, pour compenser les biais d'un PEA classique, l'intégration des données générées par les utilisateurs permet de prendre en compte l'échelle individuelle comme collective. Le rôle des liaisons numériques dans la socialisation secondaire engendre un impact sur la mobilisation d'un individu voire d'une communauté (Casilli, 2010).

La révolution informationnelle induite par le contenu généré par les utilisateurs (User Generated Content, UGC) est étudiée dans les domaines du marketing (revue de produits), du partage de connaissance (wikis), mais également dans son rapport avec les médias traditionnels. Ainsi dès qu'un journal ajoute une version en ligne permettant à ses lecteurs de générer du contenu, on remarque une différentiation avec la ligne éditoriale (Yildirim et al., 2013). L'UGC modifie totalement l'accès aux masses à l'information disponible sur un évènement donné. Au lieu d'un nombre limité de médias, tous les témoins directs et indirects peuvent générer des informations sur les évènements, le tout en temps réel.

Parmi les sites à contenu générés par les utilisateurs les réseaux sociaux se distinguent avec plus de 1,6 milliard d'utilisateurs dans le monde, dont plus de 64% ont accès à des services de médias sociaux en ligne (Statista, 2019 a). Une des principales raisons pour lesquelles les personnes utilisent les réseaux sociaux est de se maintenir informé sur des évènements en cours (Whiting et Williams, 2013). D'ailleurs « *Le contenu textuel généré par les utilisateurs a eu un impact précoce, en particulier dans le domaine de l'information et du journalisme, où le journalisme citoyen dirigé par les utilisateurs constituait à la fois un défi pour les médias grand public établis et une source supplémentaire de contenu de témoins oculaires, en particulier dans le contexte des informations de dernière minute.*» (Bruns, 2016). Ce qui entraîne un premier travers observé sur de nombreuses études : l'homophilie. L'homophilie est un fait tellement évident que des communautés entières sur Facebook peuvent être modélisées en extrapolant à partir de seulement 20% de leurs membres (Mislove et al. 2010).

Or, l'homophilie contribue à la mobilisation en impactant les quatre piliers de celle-ci tels que définis par Charles Tilly : la valeur de la cause, l'unité des membres, le nombre, et la détermination.

La prise en compte du User Generated Content (UGC) dans l'étude d'une mobilisation permet de comprendre quel type de sociabilité est en jeu dans les situations de crises, de désastres, de conflit. Intégré dans le cadre d'un PEA, l'UGC montre un autre point de vue que celui des médias, la prise en compte d'une autre partie prenante au conflit : le peuple. Certes elle vient avec ses biais et ses tropismes, mais cela reste une fenêtre sur le peuple, sur l'acteur-citoyen connecté. Dans les moments de crise, ce dernier s'empare d'un média numérique à sa disposition, et il bénéficie d'une éducation numérique suffisante pour s'en servir à bon escient. De plus, cette utilisation du média numérique vient augmenter le catalogue du répertoire de l'action collective en ajoutant une composante transnationale et homogène vu que le cadre numérique reste dicté par la plateforme utilisée plus que par le contexte de son utilisation.

Le premier apport de l'UGC au PEA est la compensation du biais de sources. En ne prenant comme source que la presse, et même en croisant plusieurs médias internationaux, le chercheur se focalise sur les acteurs officiels, majeurs, institutionnels qui sont l'objet d'attention des médias. Or : « *les données de médias sociaux offrent des avantages uniques en tant que source de données pour la détection de évènements d'action dans les régimes autoritaires parce qu'ils fournissent des informations lorsque d'autres sources, telles que les médias traditionnels, sont silencieuses.* » (Zhang et Pan, 2019).

Dans le cadre d'un conflit constitué, l'étude du média social numérique permet d'observer le comportement de ses utilisateurs. Ce comportement dépend de la plateforme employée. Plutôt que d'envisager un média social comme une source unique il est également possible de le prendre en compte strictement comme un médium entre autant de sources qu'il y a d'émetteurs et un public indéterminé. Mais pour cela il faut en définir les biais, l'unité d'encodage, et l'unité de mesure avec la même rigueur développée par les praticiens du PEA dans le contexte particulier de la guerre de l'information.

Avec les adaptations suggérées, le « protest event analysis », c'est-à-dire l'étude des évènements pour comprendre une crise est une méthodologie parfaitement transposable dans les pratiques du renseignement. Par ailleurs elle se prête particulièrement bien au traitement assisté par ordinateur, voire automatisé.

1.4. Prédire les insurrections, état de l'art en général et en situation de conflit en particulier

Il ne fait plus aucun doute que le renseignement ait un besoin avéré d'améliorer ses capacités d'exploitation des données. Ce besoin se fait de plus en plus pressant au vu de sa présence croissante dans les documents cadrant le développement capacitaire de nos forces armées.

Dès le livre blanc sur la Défense Nationale 2013, le renseignement fait partie des priorités : « *Un effort particulier doit donc lui être consacré pour la période à venir, qui devrait concerner à la fois les ressources humaines et les capacités techniques de recueil et d'exploitation des données.* ». (Commission du livre blanc sur la défense et la sécurité nationale, 2013). S'il n'est pas fait mention de méga données (big data) dans le texte, il y est clairement indiqué que le traitement des données fait partie de l'axe d'effort. La loi de programmation militaire (n° 2013-1168 du 18 décembre 2013) qui suit érige en priorité pour la période 2014-2019 l'exploitation et le traitement des données de renseignement. (Assemblée Nationale, 2013b). Il faut attendre quatre années pour que le concept de big data soit mentionné dans la revue stratégique de défense et de sécurité nationale publiée en décembre 2017, comme une opportunité intuitivement associée aux réseaux sociaux et à l'internet des objets : « *L'hyperconnectivité, les technologies du big data, l'Internet des objets et la robotique sont quelques exemples d'opportunités majeures pour la défense*.», mais aussi comme un défi : « *Nous devrons également relever le défi de l'exploitation et de l'analyse de volumes de données en croissance exponentielle [] Un effort particulier sera porté sur l'aide augmentée à l'analyse du renseignement (Big Data, intelligence artificielle).* » (Ministère de la Défense, 2017). D'ailleurs, cette revue stratégique coïncide avec le lancement du programme ARTEMIS (Architecture de traitement et d'exploitation massive de l'information multi-source) de la DGA en novembre 2017 dont l'objet est la gestion des données de masse pour pouvoir mutualiser des capacités de recherche, développement et exploitation de l'intelligence artificielle au profit des armées (Ministère de la Défense, 2018 a).

Le rapport Villani publié en mars 2018 fait de multiples mentions à la spécificité du traitement de l'information. Pour la première fois le flagrant décalage entre capacité de collecte et capacité de traitement du Big Data est mis en évidence : « *Le volume de données produites croît exponentiellement, la précision et la granularité des données produites par les capteurs*

augmentent et cette tendance ne va que s'accentuer avec le temps. Avec les ressources humaines disponibles, quand aujourd'hui on parvient à traiter une quantité de données qui avoisine au mieux les 20 %, à terme ce sera probablement moins de 2 %. » (Villani, 2018).

À ce titre, l'année 2018 marque un tournant dans la prise de conscience de l'urgence de la situation, comme le stipule le rapport annexé au projet de loi qui met en exergue l'exploitation des données, la qualifiant à la fois comme un enjeu majeur, nécessitant un effort crucial, méritant une attention vigilante. (Ministère de la Défense, 2018b).

La solution à ce défi de l'exploitation est toute trouvée, comme l'indique le projet de loi relatif à la programmation militaire pour les années 2019 à 2025 du 8 février 2018, dans le cadre de la poursuite d'effort en faveur du renseignement : « *En outre, la nécessité de sécuriser, de traiter et d'exploiter les flux d'informations, en croissance exponentielle, est facilitée par le recours à l'intelligence artificielle.* » (Assemblée nationale, 2018a). L'importance de cette capacité d'exploitation est soulignée plus encore par Guillaume Poupart, directeur de l'agence nationale de la sécurité des systèmes d'informations qui lors d'une audition devant de la commission des affaires étrangères, de la défense et des forces armées du Sénat prévient : « *Ceux qui dirigeront le monde demain sont ceux qui seront capables de posséder les données et de savoir comment les traiter. Renoncer au traitement des données nous condamne à être des vassaux. Le temps presse.* » (Sénat, 2018).

La France, au travers de ces documents de référence exprime très clairement son souhait d'intégrer l'intelligence artificielle à son arsenal pour le renseignement. Elle en a fait une priorité stratégique. Reste à traduire cette volonté en programmes de recherche et de développement. L'intelligence artificielle serait donc le remède miracle pour résoudre le problème de l'exploitation des données pour le renseignement militaire, mais qu'en est-il de son utilité pour l'anticipation : « *La fonction stratégique « connaissance et anticipation » doit permettre aux décideurs politiques et militaires de disposer, le plus en amont possible, d'éléments pour la prévision et l'action. C'est l'une des clés de l'autonomie stratégique nationale.* » (Ministère de la Défense, 2010).

Il existe de nombreux cas d'usage d'étude d'exploitation des données de masse pour le renseignement de situation au moyen d'intelligence artificielle. Un champ en particulier a été largement couvert par la recherche américaine : la prédiction d'insurrection.

L'approche centrée sur l'individu est au cœur des opérations de contre-insurrections depuis les campagnes du maréchal Lyautey en Indochine en 1895 jusqu'aux opérations américaines en Irak et Afghanistan en 2014, reprenant à leur compte le mantra « hearts & minds » stipulant

qu'il faut conquérir le cœur et l'esprit des populations parmi lesquelles se cachent les insurgés et opèrent les troupes US. Or parmi les constats retenus par le lieutenant-colonel Valeyre dans son étude historique du principe, deux d'entre elles ont eu, d'après nous ont eu une influence sur le recueil et l'exploitation de l'information au moyen d'intelligence artificielle prémices à la prédiction :

- « *Le concept opératoire d'une contre-insurrection ou contre-rébellion « centrée sur les populations ». Il suppose d'agir dans le sein de populations civiles, sur celles-ci et au bénéfice de celles-ci, en phase de stabilisation.* » (Valeyre, 2012).
- « *L'action dans le sein des populations permet le recueil de renseignements fiables, utiles à l'élimination des cellules politiques de l'ennemi. Ils permettent de loger et de retourner les combattants insurgés. Par ailleurs, la collecte de renseignements d'ambiance, de nature ethnographique ou culturelle aide les forces à maîtriser leur environnement humain.* » (ibid.).

Faisant état d'un « *nouvel appel à la prédiction en sciences sociales* » dans leur étude portant sur la prédiction du soutien civil aux insurgés afghans pour prédire le déploiement d'engins explosifs improvisés (EEI), Kentaro Hirose, Kosuke Imai et Jason Lyall concluent que : « *Les attitudes des civils sont un facteur prédictif important de multiples types de violence des insurgés en Afghanistan.* » (Hirose et al., 2017). Par extension, des fonctions de recueil et d'analyse réalisés au moyen d'intelligence artificielle seraient en mesure de prédire les zones d'insurrection à l'échelle d'un pays en guerre. Ce point focal sur le comportement individuel et l'utilisation de base de données d'évènements passés est caractéristique des études portant sur la prédiction de crise en contexte militaire. Entre 2007 et 2014, l'armée de terre américaine finance à hauteur de 800 millions de dollars par an un programme appelé Human Terrain System dont l'une des fonctions est la prédiction de crise sans que le programme n'ait abouti à des résultats satisfaisants pour la communauté du renseignement (Price, 2017). S'ils se veulent en mesure de prédire des évènements, il paraît clair que les travaux portent sur du ciblage individuel.

Dans son article Portrait de l'intellectuel en soldat de mars 2019, Olivier Koch relate les efforts américains dans le domaine du développement de : « *logiciels de la contre-insurrection [reposant] sur des modèles comportementaux dont la conception et le fonctionnement font appel à deux types de ressources : des chercheurs en sciences sociales, qui passent au crible les sociétés autochtones, et une surveillance étroite des populations* ». Du Human Social Culture Behavior Modeling centré sur l'humain, les forces armées américaines passent à

l'Integrated Crisis Early Warning System ayant vocation à prédire les crises, projet qui est suivi de plusieurs autres projets publics comme privés centrés sur la détection de stéréotypes comportementaux pour la détection et la prévision automatisée de l'instabilité sociale en estimant que : *« prédire les insurrections implique les mêmes raisonnements de prédiction comportementale que le marketing* » (Koch, 2019).

Preuve de l'intérêt pour la prédiction d'évènement par les militaires américains, c'est un sujet largement subventionné au travers de nombreuses agences militaires américaines telles que :

- l'activité des projets de recherche avancée pour le renseignement (IARPA) dans le but d'identifier les signaux faibles, les éléments précurseurs d'une crise (Hua, et al. 2016)
- l'Agence de réduction des menaces de la Défense (DTRA) pour l'étude des réseaux sociaux du terrorisme et de l'insurrection afin de prédire l'intensité d'une insurrection (Zech et Gabbay, 2016)
- le centre de recherche de l'Air Force (Dafoe et Lyall, 2015)
- ou encore le Centre de recherche Naval sur la prédiction d'émeutes au travers des réseaux sociaux (Ning, et al. 2018).

Si la majeure partie des études mentionnées tendent à conclure positivement sur la prédictibilité des évènements conflictuels certaines admettent des limitations tels que Pilster et Böhmelt qui en cherchant à prédire la durée du conflit syrien admettent que : « *deux des variables que nous avons étudié pour les trois scénarios de prédiction, Insurrection conventionnelle et Soutien économique au gouvernement, sont essentiellement invariantes dans le temps observé.* » c'est-à-dire qu'ils ne peuvent prédire que si le modèle ne change pas (Pilster et Böhmlet, 2014). De plus la très grande majorité des modèles mis en avant par des études prenant seulement en compte la data science utilisent une approche strictement statistique qu'il s'agisse du traitement de la fréquence ou de la volumétrie d'un évènement ou encore de la caractérisation d'un évènement par la sémantique algorithmique.

Avec la puissance de recherche et de financement que les États-Unis déploient, et leur capacité à tester les développements sur des terrains en conflit avec tout type de données à disposition, comment expliquer les surprises stratégiques qu'ont été les printemps arabes ou la crise ukrainienne ? Pour nous l'erreur vient tant de l'échelle choisie : l'individu, que de l'objectif à atteindre : la prédiction. Si le résultat attendu est la capacité à anticiper des crises, des conflits, des insurrections, le point focal est le groupe d'individus qui vit l'évènement. En concentrant l'intelligence artificielle sur la détection et l'analyse d'évènements qui permettent la

compilation de base de données d'évènements qualifiés, alors la modélisation de crise sera possible tout comme la détection de tendances. Ces études basées sur des data sets publiques ou privés, ne sont pas à l'abri de critiques sur la façon dont elles sont constituées. La base de la data science repose sur la capacité à entraîner les algorithmes sur des bases de références. Sans cet entraînement il ne peut y avoir de validation de modèles.

Dans le contexte de la prédictibilité des conflits, la première étape est donc la détection d'évènement pour compiler des bases de données : « *La prédiction automatisée de crises exploite des « données d'évènement » (« event data ») constituées à partir de ce qui est et a été diffusé dans les médias transnationaux, régionaux et locaux (en presse écrite, radio et télévision).* » (Koch, 2018).

1.5. Conclusion

Parmi les missions attribuées aux services de renseignement, l'anticipation est celle qui génère le plus d'attentes, voire de fantasmes. En effet, en plus de devoir appuyer les opérations en cours, le renseignement doit également éclairer la planification des opérations à venir. De ce fait, son champ d'activité ne s'opère pas seulement en situation de guerre ouverte. L'anticipation de crises appliquée aux mouvements sociaux, ou plus exactement l'élaboration de scénarios d'évolution priorisés par probabilité de survenue, ne peut se faire sans comprendre les dynamiques sous-jacentes de la contestation. Cette capacité d'anticipation est d'autant plus importante qu'elle s'envisage aujourd'hui dans le contexte du continuum sécurité-défense qui efface la frontière entre crise intérieure et intervention extérieure comme l'illustre la plupart des interventions de l'OTAN ou de l'ONU ces cinquante dernières années. Les services de renseignement intérieur et de défense doivent donc être en mesure de comprendre les dynamiques des situations de conflit et d'en estimer le potentiel à dégénérer. Pour cela ils peuvent s'appuyer sur des décennies d'années de recherche dans le domaine des sciences humaines et sociales tout comme des sciences de l'information et de la communication. La théorie du conflit et le « protest event analysis » appliqués aux réseaux sociaux numériques peuvent tous deux contribuer à la maîtrise des informations sur un mouvement social.

2. Chapitre 2 : La nécessaire évolution du cycle du renseignement

2.1. Introduction

Comme nous l'avons vu dans le chapitre précédent, l'exploitation des données issues des médias sociaux est une opportunité pour le renseignement qu'il soit militaire ou intérieur en particulier dans le cadre d'un mouvement social.

Alors que de nombreux programmes industriels et d'État font une priorité du déploiement de l'intelligence artificielle dans la valorisation de la donnée, notamment pour le renseignement militaire, le socle sur lequel celle-ci doit reposer fait moins consensus. Pour qu'une intelligence artificielle puisse comprendre ce qui est d'intérêt pour un analyste, il faut qu'elle comprenne quelles données font sens pour une requête spécifique. Cela repose sur une gestion très précise de la donnée et des métadonnées.

Aujourd'hui le développement global d'internet rend indispensable le suivi de ses évolutions technologiques et des pratiques qui en découlent. Les forces armées en général et les services de renseignement en particulier ont su mettre en place des procédures d'exploitation de contenu rigoureuses et éprouvées au fil des opérations, au détriment d'un retard dans le suivi des développements technologiques issus du Web (essentiellement pour des raisons de sécurité des systèmes d'information). Le chapitre qui suit abordera les principes et pratiques du renseignement de sources ouvertes tels qu'ils sont conçus aujourd'hui. Nous proposerons un cycle du renseignement rénové, adapté aux nouvelles capacités qu'apportent les évolutions technologiques en matière de traitement de données. Le premier sous-chapitre expliquera quels processus sont mis en œuvre pour créer le renseignement aujourd'hui, notamment comment sont prises en compte les informations issues de l'internet. Dans un second sous-chapitre nous décrirons le contexte dans lequel ces données sont créées, collectées et exploitées, à savoir un état permanent de guerre de l'information. Enfin, le dernier sous-chapitre mettra en évidence l'apport des technologies du Web aux processus de création de renseignement afin de montrer que c'est à partir de la source et de la nature des données qu'il faut construire le système de traitement de ces données.

2.2. Principes et pratiques du renseignement

L'exploitation des données de masse est une problématique connue et constante, le volume de données produites dépassant les capacités d'exploitation. Pour le renseignement militaire, le recueil n'est plus une problématique en soi, par contre l'analyse des données à des fins d'éclairage de la décision pose un problème particulier. Par extension, les capacités de création et de recueil de contenu dépassant aujourd'hui toute forme de capacité de traitement humain, l'analyste dispose donc d'une vue partielle des éléments dont il dispose réellement pour effectuer une synthèse. L'exploitation des données issues des sources ouvertes s'inscrit dans cette problématique.

En France, la veille sur le Web fait partie d'un concept global appelé « intelligence économique ». Ce terme est particulièrement complexe à définir, au point que, dans son rapport sur le sujet, le député Bernard Carayon joint en annexe une liste de 22 définitions du concept (Carayon, 2003). La volonté française de distinguer les concepts liés à l'intelligence économique des principes qui régissent le renseignement militaire est une des causes de la difficulté à les définir. Les Anglo-Saxons ne s'embarrassent pas de tels préjugés et les termes de « business intelligence » et « competitive intelligence » font sans aucun doute référence au concept d'« intelligence » dans le sens de « renseignement ».

Les sujets sont en effet parfaitement fongibles, la plupart des formations sur le domaine de l'intelligence économique se basent par sur une variante du cycle du renseignement : expression de besoin, recueil d'information, analyse, diffusion ; quand les Armées ont pour sujets d'étude ces conceptions du processus du processus de renseignement : la communication opérationnelle (communication de crise) et les opérations d'influence (lobbying). Mais ces processus sont tout à fait semblables, par exemple, le livre blanc « Regards croisés sur la veille » mentionne au moins cinq fois la description du cycle du renseignement (Alloing et al, 2011). Il n'est pas question ici d'aborder le débat sur l'origine militaire ou civile des différentes pratiques, le fait est que les deux mondes évoluent constamment pour s'adapter à un environnement changeant et chacun s'inspire des pratiques de l'autre.

Ainsi chaque activité d'intelligence économique a son pendant militaire : la veille sur le Web et autres sources ouvertes correspond au renseignement de sources ouvertes (ROSO, OSINT en anglais). Si dès les années 40, au moyen du « Foreign Broadcast Intelligence Service » américain et du « Summary of Foreign Broadcasts » britannique, les forces armées maîtrisaient

les sources ouvertes de l'époque (presse, télédiffusions et radiodiffusions), elles n'ont pas su aujourd'hui adapter leurs connaissances, quand elles ne les ont pas perdues, au recueil d'information sur internet (Schaurer, Störger, 2011).

Cadre stratégique définissant les capacités et missions de la Défense Nationale, le livre blanc de 2013 met en avant la fonction « anticipation et connaissance ». Cette fonction permet une « *appréciation libre et autonome* » ainsi que « *l'anticipation stratégique* », elle est une « *condition de l'efficacité opérationnelle* ». Le renseignement, quant à lui, « *joue un rôle central dans [cette] fonction* ». Un autre point est mis à l'honneur, il s'agit de l'exploitation d'internet à des fins de renseignement par la mise en œuvre « *d'outils spécifiques d'analyse des sources multimédias* » (Commission du livre blanc sur la défense et la sécurité nationale, op. cit.).

Cette prise en compte au plus haut niveau de l'État appelle à la mise en place d'un nouveau cycle de création de renseignement bénéficiant de l'état de l'art dans le domaine de l'exploitation de contenu.

Bien que largement financé, à l'origine, par les forces armées américaines (Sterling, 1993), les agences de renseignement ont mis beaucoup de temps à prendre en compte internet et surtout le Web comme source d'information légitime. A titre d'exemple, même si les premières informations sur le Web furent disponibles à partir de 1992 et de nombreuses unités militaires américaines disposèrent de sites internet. Pourtant, le premier centre américain dédié au recueil sur sources ouvertes (dont internet) fut mis en œuvre seulement en 2005. Il a fallu pour cela, entre autres causes, la surprise stratégique des attentats du World Trade Center en 2001 et la recommandation n°30 du rapport de la commission d'enquête qui mentionne la création d'une agence nationale d'exploitation des sources ouvertes (Zelikow, 2011). Le recours systématisé aux sources ouvertes était jusque-là freiné par le manque d'intérêt des services de renseignement pour des informations librement accessibles et par la valeur supérieure attribuée à des éléments recueillis par des capteurs confidentiels basée le coût supérieur d'acquisition qui s'agisse d'un coût humain, financier, ou en termes de risques (Schaurer, Störger, op. cit.). Cependant, malgré l'absence initiale de structures officielles, le Web en tant qu'une des parties les plus visibles et accessibles d'internet, représente une telle source de données, d'informations et de renseignements que les services s'en sont servis dès sa mise au point. C'est le cœur de sujet du renseignement de sources ouvertes (ROSO) qui depuis une dizaine d'années, tout en prônant une prise en compte globale de l'ensemble des vecteurs libres d'accès, se concentre sur l'exploitation d'internet.

Le renseignement n'est pas une fin en soi. Le renseignement apporte une « *capacité autonome […] d'appréciation* », et doit « *appuyer l'engagement des forces* » (CICDE, *op. cit.*). Les Webs quant à eux renforcent toutes les fonctions essentielles à la conduite des opérations : le commandement, le contrôle, la communication, l'informatique, le renseignement, la surveillance et la reconnaissance (C4ISR). Les pratiques du renseignement appliquées à l'internet vont au-delà du simple recueil, au-delà de la surveillance, elles peuvent également interagir avec les sources de données. Par exemple, sur les forums ou les réseaux sociaux le ROSO peut être teinté de renseignement d'origine humaine (ROHUM) lorsque l'opérateur anime des avatars pour discuter avec des sources humaines. Le Web devient même un théâtre d'opérations sur lequel sont menées des actions sur l'information et des actions de communication réunies sous le concept de « guerre de l'information » ou plus diplomatiquement dit, actions sur les perceptions et l'environnement à l'image de l'appellation de l'unité des forces armées françaises chargé de ces opérations le centre interarmées des actions sur l'environnement dont la mission est : « *Centre de référence dans le domaine de l'influence militaire (IM), il développe pour cela des moyens permettant de comprendre et d'agir sur l'environnement humain des opérations, dans les champs opérationnels aéroterrestres et numériques (notamment les réseaux sociaux*). » (CIAE, 2019).

Au début du Web, l'information y était statique. Il n'y avait pas de possibilité d'interaction et surtout elle était stockée dans des silos isolés les uns des autres. L'accès à ces silos dépendait de la capacité des moteurs à les identifier et de la capacité du chercheur à correctement interroger les index des moteurs. Pour pallier en partie ce manque de connaissance, l'OTAN, dès 2001, édite une série de trois manuels portant sur l'exploitation de l'internet à des fins de renseignement. Ces manuels ont fait la promotion de l'utilisation du Web comme source d'information, essentiellement par la description des informations qu'il était possible d'y trouver et par celle des différents vecteurs par lesquels circulent l'information : mailing-list, newsgroup, chat, etc. Si ces vecteurs sont toujours utilisés, ils ont depuis été supplantés par les réseaux sociaux numériques qui concentrent les masses d'utilisateurs de l'internet aujourd'hui.

Les manuels s'attachent à décrire les intérêts spécifiques des informations trouvées sur internet par rapport à celles obtenues par des capteurs confidentiels comme les écoutes, l'imagerie spatiale ou encore le renseignement d'origine humaine. La première particularité de l'information d'origine sources ouvertes est qu'elle n'est pas protégée. Elle peut donc être partagée à la fois au sein d'une coalition disparate en opération extérieure, mais aussi avec des

pays aspirant à rejoindre l'OTAN (Otan, 2001). La deuxième particularité mise en avant est la disponibilité de l'information. Internet est accessible à tous. La majeure partie des besoins en informations peut être obtenue par le demandeur via internet sans l'intervention des services de renseignements qui peuvent se concentrer les informations non disponibles sur internet. Enfin, le renseignement de source ouverte est vu comme un complément idéal aux autres méthodes d'acquisition d'information (interception, imagerie, filature, etc.). Par exemple, on peut fouiller l'internet et les réseaux sociaux ludiques ou professionnels pour identifier à distance des sources humaines d'intérêt qui seront ultérieurement traitées sur le terrain par des agents dans le cadre du renseignement humain (ROHUM).

Ces manuels de l'OTAN, datant de 2001 et 2002, recommandaient de suivre strictement le cycle du renseignement sur les sources disponibles sur l'internet en y apportant quelques spécificités ayant attrait à : la recherche de sources ; l'identification et la caractérisation de sources : qui dit quoi, pourquoi, et où ; et la cotation de l'information.

Les nouveaux risques liés à ce nouveau média qu'est le Web sont clairement identifiés dès le début. En premier lieu, considérant que tant que l'adresse HTTP d'un site (gisement d'information) n'est pas identifiée ce dernier ne sera pas accessible, les manuels multiplient les conseils sur l'utilisation des fonctions avancées des moteurs et des annuaires. En second lieu, la pratique du pseudonyme et de l'avatar, immédiatement employée sur les gisements précurseurs qu'étaient les newsgroups, au moment où le Web était encore une sous-culture, rendait particulièrement complexe l'identification de la source de l'information (Otan, 2002 a). Distinguer la source primaire d'une source secondaire était particulièrement difficile et dans le cas d'une source anonyme, la raison de son manque de transparence devait être déterminée. L'effort initial portait sur la localisation des serveurs grâce à une recherche sur les Domain Name Server au moyen des Whois et Traceroute puis à la manière d'une évaluation de livre, l'effort portait sur l'identification de l'auteur, l'éditeur, et le vecteur de transmission. Enfin, la cotation de l'information était basée à la fois sur les éléments d'identification et sur des éléments de contexte et de contenu : légitimité, autorité, précision, objectivité, actualité, couverture. La capacité de manipulation et d'intoxication des sources non identifiées et la saturation d'information sont affichées comme les plus grandes restrictions dans l'emploi de l'internet en tant que source d'information (Otan, 2002 b).

Ces pratiques, notamment l'emphase sur la localisation des serveurs et la recherche de sources (gisement) sont à remettre dans le contexte du Web initial où les moteurs n'indexaient que 16% d'un Web estimé à 6 téraoctets (Lawrence, Giles, 1999) contre 5 millions de téraoctets en 2004

(Schmidt, 2005). Les sites étaient isolés les uns des autres, difficilement accessibles et peu nombreux, d'où un objectif d'exhaustivité de recueil du Web utile. Le développement exponentiel du Web a rendu d'autant plus complexe la réponse aux problématiques initiales, qu'il a apporté son lot de problèmes nouveaux, tout en contribuant à doter les services de renseignement de nouvelles capacités.

Le Web est devenu un grand égalisateur de moyens, comme l'illustre le fait que les trois manuels de référence de l'OTAN sur l'OSINT ont été largement diffusés sur le Web donnant ainsi à tout adversaire potentiel une formation dans l'exploitation de l'internet à des fins de renseignement. Depuis les moyens de communication du Web initial (forum, newsgroup, mail) au moyen de coordination collective du Web social, chaque conflit des 10 dernières années s'est déroulé en partie sur les Webs (initial, social, sémantique).

Les technologies des Webs depuis l'émergence du Web social marquent un point de rupture significatif dans le déséquilibre de moyens jusque-là à l'avantage des services et forces armées étatiques. Elles mettent à disposition de toute organisation des capacités essentielles à la conduite d'opérations de grande envergure (tant géographique que temporelle), capacités connues par les militaires occidentaux sous l'acronyme C4ISTAR pour computerised command & control, communications, intelligence, surveillance, target acquisition, and reconnaissance soit commandement et contrôle, transmissions, renseignement, surveillance, acquisition de cible, et reconnaissance assistés par ordinateur.

La nature des Webs requiert des méthodes d'interactions différentes. Les services de renseignement s'adaptent au comportement des auteurs. Ainsi au recueil passif du Web initial s'ajoute désormais une interaction avec les sources du Web social que cela soit pour orienter un débat d'experts sur un forum ou pour se faire intégrer à un cercle d'amis dans un réseau. Cette pratique relève pourtant d'un autre type de renseignement, le renseignement d'origine humaine, défini comme du renseignement recueilli et fourni par une source humaine (OTAN, 2009) qui nécessite des compétences spécifiques au traitement de sources humaines afin de l'orienter de façon consciente ou inconsciente. Un exemple de cette évolution du ROSO est l' « Open Source Center »créé en 2005 au sein de la CIA. En 2006, ce centre avait pour mission de recueillir, traduire, condenser afin de le rendre exploitable tout élément de sources ouvertes susceptible d'intéresser le gouvernement américain (Minas, 2010). Il s'agit d'effectuer du ROSO « stricte » c'est à dire ne recueillir sur les Webs que des informations libres d'accès, celles-ci pouvant être de deux natures : une minorité d'informations fournies par des personnes inconscientes de leur valeur et une multitude d'informations de faible valeur individuellement,

mais de grand intérêt collectivement (principe de la longue traîne). Aujourd'hui les prérogatives du centre vont bien au-delà. Il a pour nouvelles attributions d'étudier, par exemple, le niveau de pénétration de l'internet dans les pays émergents, ou encore les pratiques dans l'utilisation des médias sociaux pays par pays (U.S. State Department, 2011).

L'exploitation du contenu d'un document, afin qu'il soit pris en compte pour produire un renseignement, est le fruit d'un processus de transformation au sein du cycle du renseignement trop souvent simplifié à une représentation en quatre étapes successives : expression de besoin, recueil des données, analyse, diffusion.

Cette vision du renseignement est largement critiquée et s'avère réductrice, loin du travail effectivement réalisé par les services. D'une part, elle propose un cadre trop rigide où l'information ne serait prise en compte que si elle permet de résoudre une question initiale (Treverton, Agrell, 2009). D'autre part, la réalité du processus cognitif induit dans l'exploitation des informations au sein d'un cycle de renseignement révèle une structure en forme de Web (Phythian, 2013) où la création de connaissance se fait par la mise en relation de documents d'origines variées et multidisciplinaires (rapport évènementiel, connaissance interne, feedback, etc.).

Par exemple, au sein du processus de renseignement militaire français, l'accent est mis sur une procédure d'affinement de l'exploitation de contenu, de la donnée à l'information, de l'information au renseignement : la donnée est la transcription d'un fait, une mesure. L'information est une donnée ayant un sens et mise en forme pour être communiquée. Enfin le renseignement est un produit de fusion et d'analyse répondant à un besoin exprimé (CICDE, op. cit.). Le sens du contenu d'un document sera exploité selon une série de filtres sur quatre niveaux, de N0 à N3 (Ministère de la Défense, 2003). Le niveau 0 (N0) est celui de l'information brute. Un document passe au niveau 1 (N1) dès qu'il est sélectionné par un analyste, c'est à dire, dès qu'un analyste se l'approprie et l'intègre dans un corpus de document susceptible de répondre à un besoin en information. Le niveau N2 est créé par la fusion des éléments N1 : c'est le moment où le sens du contenu d'un document quitte le document initial pour être assemblé avec d'autres au sein d'un document composite. Le niveau N3 est essentiellement un niveau de validation, celui des synthèses commentées de documents de niveau 1 ou 2. Dans la mesure où elles sont estimées comme répondant à un besoin en information pouvant être transmises au demandeur, elles sont validées et classées « niveau 3 ». Le cycle le plus représentatif des processus mis en place dans la création d'un document N3 peut être adapté de celui de Geraint, où le rôle central, ici joué par l'intention du commandement

et la prise en compte de l'environnement opérationnel, est remplacé par une base de connaissances.

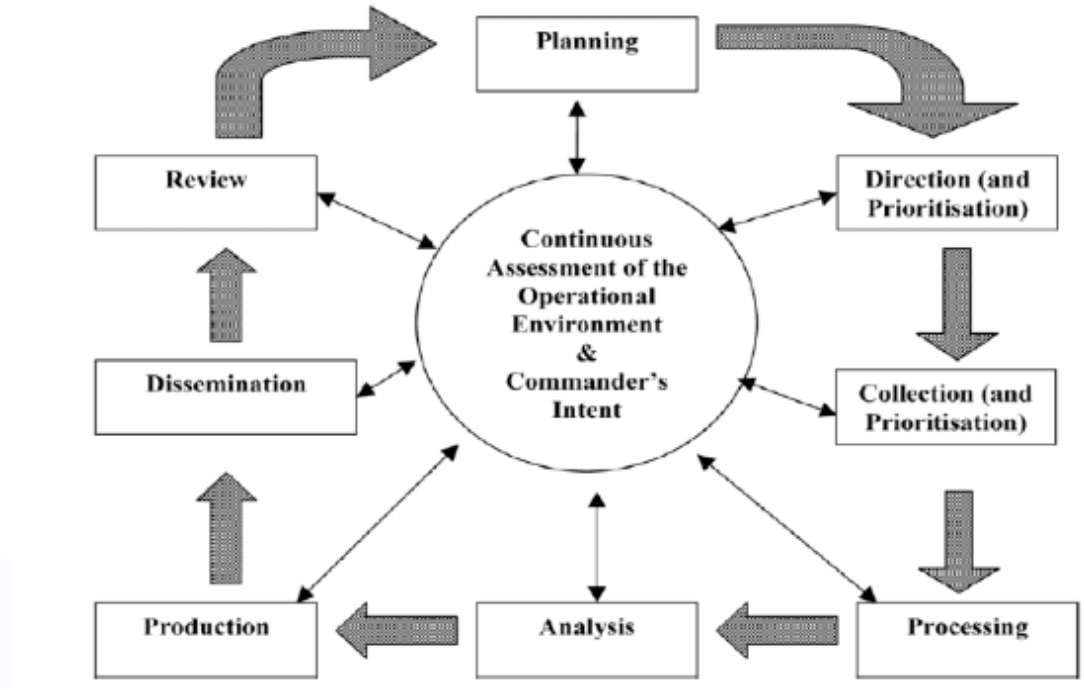


Figure 1 : Cycle du renseignement (Geraint, 2009)

Sans être parfait, le cycle de Geraint a le mérite d'illustrer les nombreux échanges qui alimentent un processus d'exploitation. Ce type de schéma place comme seule impulsion du processus d'exploitation une demande initiale aux fins de planification. Or un renseignement peut être créé en interne à seule fin d'enrichissement ou mise à jour des connaissances au sein d'un cycle de capitalisation. Autre critique, le recueil et l'analyse se font le plus souvent de façon concomitante et non successive. La représentation mentale de la forme de la réponse à la question initiale évolue au fur et à mesure du recueil de documents, réorientant ce recueil en fonction du besoin au sein d'un cycle d'exploitation (Hulnick, 2006).

Le cycle du renseignement est en fait un ensemble d'engrenages concentriques dans la mesure où chaque grande étape (Expression de besoin, Recueil, Analyse, Diffusion) est subdivisée en processus cycliques successifs interdépendants. Au centre de cette cascade d'engrenages se trouve une fonction de gestion des connaissances de l'organisme dont le rôle est d'animer l'ensemble des cycles. Dès aujourd'hui, une base de connaissances peut tirer parti d'avancées majeures en termes de gestion de connaissances que sont le tagging social, la navigation

facettée, le filtrage collaboratif, etc. (Marlow et al, 2006). Le concept interarmées n°2 portant sur le renseignement d'intérêt militaire (CICDE, 2009) donne pour définition de la connaissance : « *élaboration de l'information ou d'un ensemble d'informations mises en relation, par l'intermédiaire du jugement ou du discernement de la personne qui définit cette connaissance, en recourant si nécessaire à l'interprétation* ».

La connaissance se distingue alors du renseignement dans la mesure où un renseignement répond à un besoin alors qu'une connaissance est générée au fur et à mesure de l'évolution du savoir d'un analyste sur un sujet. Le Knowldege Development (création de connaissances) est une fonction essentielle du renseignement, car elle seule permet l'anticipation par l'identification des signaux faibles et la fusion multisources « proactive » c'est-à-dire une fusion libre et prospective, qui ne dépend pas d'une orientation initiale. La réflexion doctrinale sur le sujet en France porte essentiellement sur des schémas de collaboration interservices, mais n'aborde pas l'aspect technique qui est à la fois nécessaire et déjà possible à déployer (CICDE, 2010).

Les progrès technologiques du Web social entraînent une perte du contrôle de l'information disponible qui ne peut être compensée que par la sensibilisation (Délégation à l'Information et à la Communication de la Défense, 2012). Cependant, s'il y a une leçon à retenir des actions de renseignement sur le Web social c'est que le Web offre tous les jours de nouvelles capacités, indistinctement, tant aux services les plus respectables, aux combattants pour la liberté qu'aux terroristes. Chaque nouvelle possibilité a son pendant négatif, sa faille de sécurité. Le taux de pénétration d'internet au sein des zones de crises potentielles est en rapide augmentation (Délégation aux Affaires Stratégiques, 2013). L'accès à internet est considéré par les nations occidentales comme un droit fondamental. Pour contrer le strict contrôle mis en place par des régimes autoritaires (Kelly et al., 2013) de nombreuses inventions permettent de déployer un réseau internet par satellite, avion et aérostat (Google, 2013) et ce malgré la volonté d'un État hostile à sa diffusion. Plus le Web sera disponible, plus le potentiel de renseignement sera développé.

Le renseignement de sources ouvertes complète de multiples façons la fonction renseignement. Il met à disposition de nouvelles sources et de nouvelles pratiques, complémentaire à l'existant.

2.3. Information/désinformation dans la guerre de l'information

Les deux domaines, ROSO et cyber guerre, sont des problématiques et des centres d'intérêt pour les entreprises. Grâce à la conjugaison d'une plus grande expertise et surtout de meilleurs financements, celles-ci recueillent, luttent et surtout développent avec une grande réactivité des outils pour améliorer leurs capacités dans ces champs d'action. Ainsi les adversaires des forces étatiques ont désormais accès non seulement à ces mêmes capacités, mais en plus à des moyens de communication des plus immédiats et visibles (Twitter, au moyen de comptes à usage unique) aux plus discrets (boîte mail partagée évitant la transmission de message). Ces technologies leur donnent notamment les moyens d'alerter leur commandement ou de transmettre à leur communauté des éléments d'intérêt, de partager une image tactique en temps réel (diffusion de position de troupes), de diffuser des ordres, de synchroniser des opérations. Les adversaires irréguliers auxquels sont confrontés les services de renseignement ont désormais à leur disposition de l'imagerie satellite haute définition, un accès à des banques de données confidentielles, et des moyens de renseignement d'origine humaine à la fois sur les théâtres d'opérations et sur le territoire national d'origine des troupes qu'ils affrontent.

Le Web initial a évolué vers le Web social et les pratiques des services de renseignement s'y sont adaptées. Comme décrit dans la première partie de ce chapitre, parmi les particularités de ce Web sont essentiellement : une interaction avec l'information via les commentaires, une explosion du volume de contenu et les réseaux relationnels comme nouveaux vecteurs de diffusion. Les évolutions technologiques apportées par ce Web permettent de répondre à quelques problèmes des services de renseignement sur le Web initial. Les moteurs de recherche deviennent de plus en plus exhaustifs. La navigation facettée (c'est-à-dire la sélection des résultats par des critères autres que la correspondance stricte à la requête initiale) au sein de leur index est plus pertinente pour l'utilisateur. De plus, le maintien de l'anonymat requiert une haute compétence technique. Les nouveaux vecteurs de diffusion deviennent des facilitateurs de la création de contenu, tout utilisateur devenant un auteur potentiel. Ce créé ainsi un écosystème informationnel doté de nouvelles propriétés intéressant les services de renseignement :

- l'immédiateté de la diffusion : le twittos (utilisateur de Twittter) Sohaib Athar commente en direct une des opérations les plus secrètes de la décennie, l'assaut sur la demeure de Ben Laden à Abbottabad (Pakistan) par les forces américaines, c'est-à-dire

une intervention étrangère dans un état souverain non coopératif (Sohaib Athar, 2011). Autre exemple d'apparence plus anodine, les spotters passionnés d'aéronautique ou de construction navale qui diffusent toutes photos des différentes étapes d'essais de prototype en cours de développement.

- le commentaire de l'information : toute déclaration publique officielle, de quelque autorité que ce soit, est soumise à une critique en temps réel. Des sites de fact-checking (pratique journalistique de vérification des déclarations publiques) et d'explication de situation apparaissent sur tous les sujets d'actualité militaire, par exemple le site Web Syria Deeply se veut neutre et exhaustif sur la crise syrienne (Syria Deeply, 2013).
- le profilage d'individus, étude des réseaux relationnels soit à des fins de ciblage pour être traités en tant qu'interlocuteurs ou pour élimination. Toute l'activité d'un individu ou d'un réseau sur le Web, sites visités, tags employés, commentaires émis permet d'en dresser un portrait des plus fidèle. Très utile en début de crise, les réseaux sociaux permettent par exemple le suivi d'activistes de l'opposition. Ils ont permis aux services de renseignement de suivre le développement du Printemps Arabe, plus particulièrement d'en mesurer l'ampleur et l'irrévocabilité.
- l'interaction avec les acteurs sur place, par exemple en Libye à défaut d'autres réseaux disponibles les alliés libyens de l'OTAN annonçaient la position de leurs chars pour éviter les tirs fratricides (CICDE, 2013 a), voire utilisaient Twitter pour transmettre des positions de cible et des évaluations de dégâts après les bombardements (Bradshaw, Blitz, 2011).
- la participation collective au renseignement, par exemple, des projets initiés pour des raisons caritatives comme satsentinel.org utilisent des collectes de fonds pour financer de l'imagerie spatiale permettant d'apporter des preuves d'actes de guerre contre des populations civiles. L'imagerie mise à disposition par ces projets est de haute qualité et son analyse d'une grande précision, faite par des centres universitaires et avec l'appui de militaires à la retraite (Satsentinel, 2013).

Ces adversaires s'avèrent tout aussi compétents dans l'exploitation de ces éléments mis à disposition. Du film de combat posté sur Youtube par un soldat révélant les tactiques et le matériel employés aux photos sur Facebook incluant la géolocalisation, les médias sociaux sont une mine pour les adversaires de ces troupes amenées à être composées essentiellement de «digital natives», individus nés à partir de 1990 et baignant dans la culture d'internet et les nouvelles technologies de l'information et de la communication. Ainsi, en 2010, le Hezbollah

avait réussi à être « l'amie » d'environ 200 soldats des forces spéciales israéliennes au moyen d'un faux profil sur Facebook (Stricker, 2010). En 2011, des activistes ont réussi à faire le lien entre les annonces de sécurité d'un service de trafic aérien maltais (pour écarter le trafic civil des zones dangereuses) et les frappes de l'OTAN sur le territoire libyen. En 2012, une mère publie des informations portant sur une manœuvre de guerre électronique en Afghanistan sur une liste de diffusion Yahoo (Hecker et al, 2012). Le droit d'accès à l'information offre les ordres de bataille complets des unités et des renseignements sur les programmes d'avenir. La liberté d'expression et les indiscrétions à la presse qui en résultent sont diffusées immédiatement sans contrôle d'accès possible. L'accès à l'internet en tant que droit fondamental s'appliquant évidemment aux soldats en opération, il est régulièrement source d'indiscrétions. Ces dernières années, lorsque l'internet est mentionné dans une problématique militaire, il est immédiatement associé au concept de cyber défense. Il existe une profusion d'études, de lois et doctrines traitant de la cyber guerre en cours et à venir. Chaque gouvernement ou organisation multinationale (ONU, OTAN, UE) présente cette guerre sous la forme d'une lutte informatique défensive et offensive, se traduisant par l'affrontement entre des hackers (étatiques ou non) et les défenseurs d'un ensemble de réseaux. Les théories sous-jacentes sont une transposition « cyber » de la lutte du boulet contre la cuirasse, et le combat s'apparente à une succession de découvertes de failles et de contre-mesures. La menace clairement exprimée à travers ces textes reste calquée sur la mémoire de conflits passés à savoir une attaque massive sur une infrastructure stratégique.

Cette focalisation sur la préservation de l'intégrité du réseau internet, indéniablement stratégique, masque pourtant cet autre niveau d'affrontement qui se déroule sur les Webs.

Le renseignement est composé de plusieurs branches dont les principales sont le renseignement d'origine humaine (conversations et observations), le renseignement d'origine image (satellites et appareils photo), le renseignement d'origine électromagnétique (écoutes et interceptions). Toutes ces capacités sont utilisées pour agir efficacement sur le champ de bataille. Or désormais celui-ci inclut les Webs. Dans les paragraphes précédents, il a été démontré que les Webs fournissaient les mêmes opportunités et les mêmes armes à l'ensemble des belligérants, or ils apportent également leurs propres combattants. En plus d'un affrontement classique entre deux ennemis conventionnels ou asymétriques, les Webs ont fait émerger un type de soldat qui leur est propre, un adversaire au potentiel de nuisance aléatoire sans ennemi prévisible. Parmi les atteintes portées aux services de renseignement deux événements récents ont eu une portée significative : l'affaire Manning et l'affaire Snowden. Les documents révélés par ces lanceurs

d'alertes internes ont fragilisé l'activité des services de renseignement sur le Web en révélant leurs pratiques et leurs cibles. De nombreuses autres affaires de ce type ont lieu régulièrement dans le monde entier et sont tout autant dommageables sans qu'elles atteignent une telle portée médiatique (l'affaire Hammond (USA) ou encore Kamm (Israël)). De multiples autres actions ont lieu quotidiennement qu'elles viennent de groupes plus ou moins indépendants, prenant la forme de la désobéissance civile numérique (Anonymous), ayant une cause libertaire ou humoristique (Lulz), et parfois même patriotique (Syrian electronic Army). Hormis la dernière catégorie, ces cyber soldats sont susceptibles d'apporter leur soutien à n'importe quel camp, à tous, ou à aucun.

Les champs de bataille modernes imposent une multitude d'opérations concomitantes, dépassant les opérations de combat sur le terrain. Les services de renseignement officiels ou irréguliers (dans le cas d'un conflit asymétrique) doivent impérativement maitriser Influence, communication, action civilo-militaire pour le succès d'une opération. Rassemblées sous le concept général « d'opérations d'information », les opérations militaires d'influence, la communication opérationnelle, et les opérations psychologiques se dérouleront de plus en plus sur les Webs. La doctrine française s'attache à décrire de façon neutre les opérations militaires d'influence, opérations visant à agir sur l'environnement psychologique de groupes alliés, adverses ou neutres afin de contribuer à atteindre l'effet final recherché. Cependant, dès les premières pages, ces opérations d'influence se mettent directement dans une position d'affrontement contre un adversaire irrégulier qui : « *[profite] des technologies de l'information et de la communication pour mener son combat avec ses propres règles* » (CICDE, 2008). Le champ de l'information est déclaré comme un « espace de combat » (CICDE, ibid.). Les missions de ce combat sont par exemple, nuire à la légitimité et la crédibilité de l'adversaire, instaurer la dissension au sein des groupes de l'opposition, identifier les opérations de désinformation et de propagande ennemies, etc. Le retour d'expérience des dernières opérations de coalitions occidentales (Irak, Afghanistan, Libye, Mali) ou d'opérations nationales (Israël, Syrie) démontre que les Webs sont au cœur de l'affrontement.

En plus de l'accès à des moyens de création de contenus et de diffusion, une autre particularité des Webs est leur capacité à déplacer l'affrontement en dehors de la zone de combat locale vers l'arrière de l'adversaire, là où il se sent le plus en sécurité, le plus légitime. Ce déplacement du combat se fait non seulement vers les populations d'origine des belligérants, mais aussi à l'échelle globale. Si pour les forces occidentales (parfois elles-mêmes divisées sur le niveau d'intervention légitime), le but est de « gagner les cœurs et les esprits » en faisant la promotion

des bienfaits de la force d'intervention, celui de leur adversaire peut être de la décrédibiliser pour en forcer le retrait par pression politique interne, par exemple au moyen de diffusion massive d'images de dommages collatéraux, victimes civiles réelles ou fictives. L'adversaire peut encore générer des attaques sur le territoire d'origine de cette force par la radicalisation d'individus sympathisants. Ainsi Mohammed Merah a justifié ses crimes comme étant des représailles à l'intervention française en Afghanistan. Cet exemple illustre la confusion des zones d'affrontement entraîné par les Webs, un combat sur un territoire extérieur devient un problème de sécurité intérieure. Nous reviendrons sur ce continuum sécurité-défense dans le chapitre 8. Les forces en présence sont contraintes d'effectuer un effort supplémentaire sur la communication nationale et globale. Il ne suffit plus de bien faire son métier, il devient indispensable de bien le faire savoir. La doctrine française portant sur les opérations civilo-militaires envisage d'utiliser les réseaux sociaux pour développer leurs contacts au sein de la population locale (CICDE, 2012). Les Webs deviennent au besoin des vecteurs de propagande, des théâtres d'opérations psychologiques, des centres de formation (n'importe qui peut être formé à la fabrication d'explosifs artisanaux sur le Web), des dispositifs de ciblage et de recueil d'informations sur des individus ou des structures (plans, photos etc.), des moyens de collecte de fonds et transactions financières. Il n'y a pas un domaine de la guerre qui n'aie son pendant sur les Webs, des effets psychologiques aux destructions d'infrastructures.

Ces capacités sont tellement efficaces et si facilement disponibles qu'elles font envisager la fermeture de réseaux sociaux tels que Facebook ou de services Webs tels que BlackBerry Messenger par ces États occidentaux qui se félicitaient de l'utilisation du Web social par les révolutionnaires du printemps arabe (Lewis et al, 2012). Par ailleurs, ces mêmes États disposent d'un arsenal législatif et technologique pour espionner leur propre population sur les Webs, espionnage révélé par des hackers ou lanceurs d'alertes au moyen de réseaux sociaux. Signe de la prise en compte de l'évolutions des environnements informationnels les doctrines et procédures du renseignement militaire changent également de périmètre. Ainsi la doctrine interarmées du renseignement de 2004, est remplacée en 2009 par la doctrine interarmées du renseignement d'intérêt militaire et contre-ingérence.

2.4. L’analyse pour le ROSO : de nouvelles perspectives

Pour mesurer la difficulté de confier à une intelligence artificielle l’appui à fournir à un analyste du renseignement militaire, il faut se poser la question de ce qui peut faire sens pour ce dernier. La notion de sens est particulièrement complexe. Il y a autant de sens attribués que de personnes qui accèdent aux données. En effet, comme le défini Pierre-Michel Ricordel : « *l’émetteur exprime un message porteur d’une signification qui n’est pas universellement définie, qui représente donc un potentiel de sens*.» (Ricordel, 1998) ce qui fait dire à François Rastier : « *le sens n’a pas d’existence propre hors de sa profération et de son interprétation.* » (Rastier, 1989). Cette notion dynamique du sens, « *produit de l’activité de l’interpréteur* » (Sabah, 1997) entraînera de grandes difficultés dans l’évaluation de la pertinence d’un document, c'est-à-dire « *le choix de l'interprétation la plus plausible dans le contexte courant.* » (Sabah, ibid.), par les intermédiaires entre l’auteur et l’utilisateur. Cette difficulté de définition du sens engendre une difficulté de création de connaissance qui s’avère exponentielle lorsque cela s’applique sur des données de masses en général et pour le renseignement en particulier.

Au-delà des approches sémantiques et pragmatiques, on peut choisir de limiter la notion de sens aux connaissances du contenu (pour les distinguer des métadonnées du contenant) pour un utilisateur défini et leurs représentations au moyen de technologies. Il s’agit de distinguer deux volontés (et les moyens d’exploitation associés), volonté de l’auteur/capteur de décrire ce qu’il a voulu exprimer et volonté des utilisateurs de décrire leurs interprétations du document, le sens intrinsèque (donnée capturée) et le sens interprété (donnée exploitée). Ainsi, une intelligence artificielle doit pouvoir appliquer ses capacités sur des données structurées pour en extraire le plus de connaissance à la fois par les données et les métadonnées.

2.4.1. L’apport du Web sémantique et de l’intelligence artificielle

Pour illustrer l’apport que les technologies du Web peuvent apporter au renseignement, nous allons prendre en compte une technologie du Web sémantique le Rich Data Format (W3, 2004). Pour donner du sens au contenu issu des médias sociaux de nos travaux, il faut être en mesure d’intégrer l’ensemble des données soit bien plus que le seul contenu d’un message (voir chapitre 4.1 : Qu’est-ce qu’un tweet ?). Tout d’abord, tous les documents conçus ou intégrés dans une base de connaissances doivent contenir l’ensemble de leur métadonnées (ce que permet le RDF). Cette technologie du Web sémantique permet le même bond en avant que le Web initial

a fait lorsqu'il a séparé les documents de leur emplacement physique, en dissociant les informations de leur support (Adrian et al, 2010). Les informations exprimées au moyen de triples, c'est-à-dire des trinômes sujet-prédicat-objet, ou encore sujet-propriété-valeur de la propriété peuvent être mises en relation les unes avec les autres avec une plus grande précision qu'une similitude de mots clefs. Ainsi, en plus d'être conçue autour d'une base de données relationnelle, une base de connaissances peut utiliser un « triple store », une base de données conçue pour gérer les triples du RDF. Un « triple store » est essentiel à la mise en place d'un wiki sémantique dans lequel toutes les entités nommées reconnues automatiquement dans un texte deviennent autant de lien vers d'autres textes les mentionnant (Semantic Media Wiki, 2013). La mise en place de ce « triple store » doit pouvoir se faire automatiquement au moyen de fouille de texte (text-mining) qui reconnaîtrait les entités nommées à partir d'un vocabulaire contrôlé.

Dans le cas du renseignement militaire, plusieurs exemples de vocabulaires contrôlés (au même sens où l'entend le concept SKOS décrit ci-après) existent déjà sous la forme de glossaires multilingues comme ceux employés par l'OTAN. Ce vocabulaire contrôlé peut ensuite être ordonné sous la forme d'une ontologie, c'est à « *une structuration des concepts d'un domaine. Ces concepts sont rassemblés pour fournir les briques élémentaires et exprimer les connaissances dont on dispose dans ce domaine* » (Bachimont, 2006) afin que chaque mot devienne un sujet auquel seront ajoutés un prédicat et un objet. De plus, de nombreuses ontologies à vocation civile présentent un intérêt militaire. C'est le cas de geonames.org qui recense plus de 8,3 millions de toponymes. D'autres ontologies peuvent avoir de la valeur par leur structure comme une ontologie portant sur des films ou encore sur des personnes d'intérêt alors même que leur contenu peut être sans intérêt. Trois concept paraissent intéressant pour la structuration du renseignement dans la mesure où ils peuvent être appliqués à l'ensemble des données d'une base de connaissances, il s'agit de la combinaison de l'ontologie Friend of a friend (description d'une personne et de son réseau), la recommandation du W3C Simple knowledge organization system (thésaurus, classifications, vocabulaires contrôlés) et Semanticly interlinked online communities (description des vecteurs d'information d'une communauté en ligne).

- Friend of a Friend, FOAF.

  Si la base des connaissances doit permettre à tout le monde de bénéficier de l'information collective, elle doit également respecter les droits d'accès à l'information protégée et gérer le besoin d'en connaître d'un analyste, ce sont deux principes de la protection des

informations classifiées de défense. Au-delà de l'exploitation des données recueillies, l'autre apport des propriétés FOAF est la protection de l'accès aux données. Par exemple, toute la fiche de poste d'une personne peut être décrite par les propriétés de FOAF puisque celles-ci sont créées au besoin qu'il s'agisse de décrire son environnement de travail : horaires « foaf : WorkingHours », subordination « foaf : superior », collaborateurs foaf : staff »), ses centres d'intérêts (permanent « foaf : CurrentProject », occasionnels « foaf : Part-timeProject », exceptionnels « foaf : SyriaCrisisGroup »), ou son besoin d'en connaître « foaf : HasAccess » ou son habilitation « foaf : SecurityClearance ». L'ontologie FOAF lui garantirait l'accès à l'ensemble de l'information nécessaire, car une fois l'organigramme de l'organisation décrit, il serait possible de créer des règles d'attribution automatique de documents en fonction de la corrélation entre les centres d'intérêts déclarés par une personne et les thématiques abordées par un document exprimés au moyen de la recommandation SKOS. Des algorithmes de machine learning peuvent également superviser l'intéraction utilisateur-document pour détecter les anomalies ou pour améliorer les résultats d'un moteur de recommandation.

- Simple knowledge organization system, SKOS (W3,2012).

SKOS permet de décrire un concept au sein de schémas de concepts (fonction schémas) via les propriétés « skos : ConceptScheme », « skos : inScheme », « skos : hasTopConcept », permet de créer des collections de concepts pour les rassembler autour de thématiques plus larges et permet même de créer des liens entre schémas de concepts (fonction de cartographie). Dans une certaine mesure, ce vocabulaire permet de préciser le champ lexical (fonction lexicale) d'un concept et d'en donner une traduction au moyen d'un binôme « skos : prefLabel » et « skos : altLabel. Le concept peut être développé « skos : broader », reduit « skos : narrower », ou encore mis en relation « skos : related » (fonction sémantique). Il est également possible d'annoter un document dans son ensemble (fonction notes), et même de suivre un historique des annotations, cette capacité est particulièrement intéressante à mettre en œuvre au sein du cycle du renseignement où un document est consulté par de nombreux analystes. De nombreux développements, notamment au sein de communautés de rédacteurs de blogs, proposent le marquage automatique de document, à l'image du plug-in PoolParty Thesaurus pour Wordpress (Moser, 2012). Identifiés par le vocabulaire SKOS, les concepts clefs, entités nommées, toponymes mentionnés au sein d'un document deviennent autant de liens vers d'autres documents les évoquant. De plus, un simple survol

de la souris sur ces liens peut générer un « pop-up » fournissant un complément d'information.

- Semanticly interlinked online communities, SCIOC (RDFS, 2010)

Troisième brique (avec les langages FOAF et SKOS) de la structure d'une base de connaissances sémantique, le vocabulaire SIOC permet de réunir l'ensemble des communautés travaillant avec la base quels que soient leurs vecteurs de communication. En effet, il est probable que l'intégration toujours plus poussée de technologies des Webs, associée à un volume de données toujours plus volumineux, entraînera l'intégration de différents vecteurs d'information au sein de l'intranet militaire voire changera même quelques pratiques dans le domaine du renseignement militaire. Les sites intranet intègrent déjà des fonctions du Web initial tels que Webmails, forums, chat, communautés de travail, wikis. Au vu de l'augmentation croissante de l'exploitation de contenus issus de sources ouvertes, il sera rapidement pertinent pour un service de renseignement, lorsque des garanties de sécurité le permettront, de mettre en place sur son intranet des moyens de diffusion et d'exploitation de photos et de vidéos (de type Flickr et Youtube) appelant des commentaires transmis via des alertes de type Twitter. La multiplication de gisements d'informations spécifiques à chaque format de document génèrera le besoin d'organiser leur cartographie et leur interconnexion.

2.4.2. Proposition pour un nouveau modèle du cycle de renseignement

Le schéma ci-après illustre le réseau que forment les cycles de création de renseignement. La base de connaissances, les processus numérotés de 1 à 6, ainsi que les cycles d'exploitation et de capitalisation sont les plus à même de bénéficier des technologies des Webs initial, social et sémantique et de l'apport de l'intelligence artificielle.

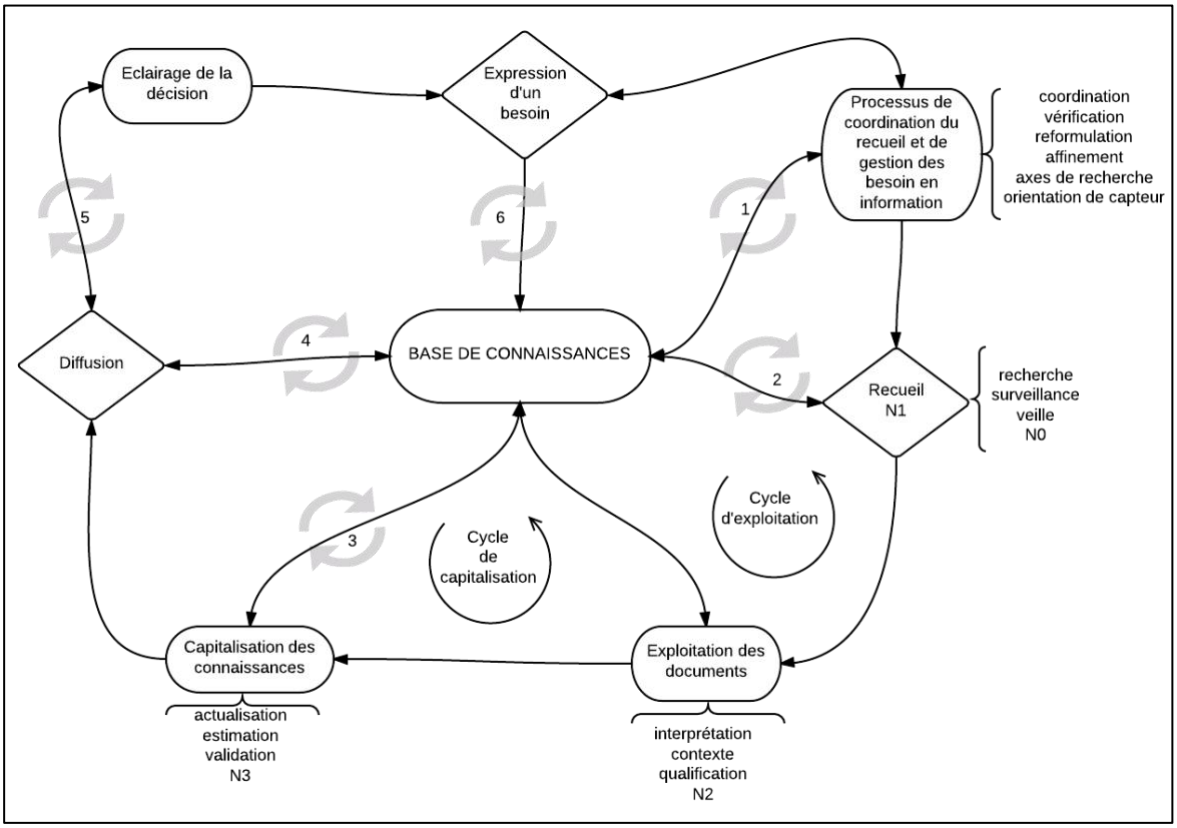


Figure 2 : Les cycles de création de renseignement

Tous les documents, du document brut de début de cycle au plus élaboré à fin de diffusion, mais aussi toutes les métadonnées des documents, convergent vers la base de connaissances. Celle-ci peut alors générer des nouvelles informations et accroître les capacités informationnelles à chaque étape grâce aux technologies des Webs. Si l'on reprend le schéma standard en quatre étapes : orientation, recueil, analyse et diffusion, dans le nouveau proposé ces fonctions sont représentées de la façon suivante :

- orientation : anticipation des besoins (processus n°6) ;
- recueil : rationalisation des abonnements, axes de veille, et ressources allouées par problématique ;

- analyse : identification de problématiques associées, de signaux faibles, automatisée par l'étude des tags attribués aux documents ; mise en perspective de l'information plus rapide et meilleure cotation de sources ;
- diffusion : étude du retour sur investissement facilitée par le ratio entre le temps, l'argent et les ressources humaines investis par rapport au niveau de satisfaction ;
- Expression de besoin.

- Expression de besoin

Première étape des cycles du renseignement, l'expression d'un besoin peut venir d'une entité extérieure à la fonction renseignement, mais aussi être générée en interne par le cycle d'exploitation pour enrichir un corpus issu d'un premier recueil. Ainsi une intelligence artificielle peut comparer des dossiers de différents pays sur de même thèmes et révéler à l'analyste des manques d'informations ou des informations contradictoires.

Cette expression de besoin peut encore être générée par le cycle de capitalisation pour actualiser un renseignement. Elle passe au filtre du processus de coordination du recueil qui, en accédant à la base de connaissances, détermine si le besoin peut être compensé par des éléments déjà existants ou si un processus de recueil doit être mis en œuvre comme indiqué par les processus n°1 de l'illustration précédente. Parmi les technologies des Webs à mettre en œuvre à cette étape le balisage (tagging) c'est-à-dire la description par mots-clefs, en particulier au moyen du vocabulaire contrôlé, est très utile. Grâce à lui, le document qu'est l'expression de besoin peut être suivi et associé à tous les documents bruts qui composeront le document composite (fusion multi sources) qui répondra à ce besoin. La description d'un document est automatisable par une intelligence artificielle supervisée par un analyste. Les différentes expressions de besoin qui partagent un même mot-clé pourront être identifiées et associées aux mêmes axes de recherche ou plans de veille. Autre technologie à mettre en œuvre est l'ontologie FOAF. Cette ontologie relationnelle structurant l'ensemble du personnel autour des thèmes traités par l'organisation permettrait de garantir de façon automatique que toutes les personnes susceptibles de contribuer à la demande en information soient informées de son existence (Breslin et al, 2011).

- Recueil

Le recueil d'information est évidemment multi-sources. L'internet n'étant qu'un capteur parmi l'ensemble des sources ouvertes que représente toute information pouvant être librement obtenue quel que soit son vecteur : publication, tract, conférence, discours public,

internet, télévision, radio, etc. (Johnson, 2009). Dans le cadre du recueil sur internet, les technologies des Webs sont utilisées à deux moments distincts, lors de la recherche de l'information et lors de la capitalisation de l'effort de recherche (processus n°2). Tous les éléments constituant l'effort de recherche sont enregistrés (temps passé, coût des abonnements, catalogue des sources veillées, etc.). Chaque source entrée en catalogue peut être étiquetée à la manière d'un signet partagé du Web 2.0 (à l'image de ce qui se fait sur le site Delicious.com) afin de la rendre identifiable par l'ensemble de la communauté en ayant le besoin (Nasirifard et al, 2010). Les documents recueillis peuvent bénéficier à l'ensemble de cette communauté et pas seulement la partie chargée de traiter l'expression de besoin. Un autre bénéfice majeur de l'application des technologies du Web au recueil réside dans les algorithmes de filtrage collaboratif à l'image du système de suggestion d'Amazon.com. Les autres utilisateurs ayant choisi tel document ont également choisi tel autre document. Le modèle d'utilisateur est la référence pour la suggestion de document, créé par la fiche de poste, il peut être affiné au moyen de data mining : fréquence et préférence de choix passés ; statistique : analyse des logs de sessions ; probabilité : étude de la navigation (Rawat, 2010). Enfin la structure en réseau des cycles du renseignement et les principes de « tagging » social faciliteraient la cotation de l'information, c'est à dire : « *l'évaluation de la véracité d'une information et de la fiabilité de la source qui l'a fournie* » (CICDE, 2010 b). L'ensemble de la communauté pourrait être mis à contribution pour déterminer si une source est totalement fiable, partiellement ou rarement, si une information est corroborée ou douteuse. Une partie de cette évaluation pourrait être automatisée. Par exemple établir des règles de cotations initiales en fonction du rapport entre la source et le sujet : différence d'appréciation de la situation sécuritaire au sein d'un camp de réfugiés dans un rapport de l'ONU et dans un rapport du gouvernement d'un pays d'accueil.

- Analyse

Le processus de sélection des éléments recueillis est la première étape du cycle d'exploitation. Dans le système français du renseignement militaire cela correspond au passage N0 à N1 d'un document (première étape sur 3). A partir du moment où un document est sélectionné, il est contextualisé. Cette étape pourrait être structurée de façon systématique par l'emploi du format Dublin Core qui regroupe les 15 éléments suivants : titre, créateur, sujet, description, éditeur, contributeur, date, type, format, identifiant, source, langue, relation, couverture, droits (Dublin Core Metadata Element Set, 2012).

Chacun de ces éléments peut constituer une facette par laquelle l'analyste peut accéder au document dans la base de connaissances, créant ainsi une multitude de chemin d'accès à l'information et la connaissance. Ainsi le système bénéficie de la sérendipité (c'est-à-dire la capacité à voir un document pertinent alors qu'il n'était pas recherché) inhérente à toute démarche de recherche d'information sur le Web. Un document trouvé peut servir à combler d'autres besoins en informations que celui qui a déclenché la procédure de recherche.

L'accès permanent à une base de connaissances bien structurée permet d'exploiter un document avec une grande efficacité accélérant les processus d'appropriation, d'interprétation et de mise en perspective de ce cycle. Les communautés de travail, rendues possibles par les outils de travail collaboratifs, ne sont plus restreintes à la lecture seule d'un document. Les documents peuvent être commentés, les photos annotées (reconnaissance faciale automatique de personnes ou de matériel) ainsi à lieu une véritable interaction avec le contenu (Rattenbury, 2007).

Une fois un document exploité et intégré dans une réponse à un besoin en information, ce nouveau document composite peut être directement diffusé à l'émetteur du besoin. En fonction de nouveaux besoins, il sera mis dans un cycle de capitalisation afin de l'intégrer à d'autres documents composites ou afin de le maintenir à jour. Le cycle de capitalisation est un cycle d'exploitation simplifié. Les documents ayant déjà été triés, validés, cotés, il consiste en une adaptation du corpus à une nouvelle demande potentielle. Ce processus (n°3) pourrait utiliser les structures de document au format XML. Les parties à mettre à jour pourraient être identifiées par un time-stamp (marquage temporel) déclenchant une alerte de péremption ou encore par une note créée automatiquement à un format différent du format initial (sans les annexes, ou avec seulement une partie d'entre elles).

Technologie typique du Web 2.0 (avec la communauté et l'Ajax) le mashup permet la fusion d'éléments de formats disparates, mais d'intérêts complémentaires. Ainsi un document composite peut être créé par la fusion d'une chronologie d'événements sécuritaires sur une carte de théâtre d'opérations (GeoConcept, 2012). Le graphe relationnel d'entités nommées dans une thématique suivie est un autre document pouvant être créé dans un cycle de capitalisation. La technologie la plus enrichissante pour un cycle de capitalisation pourrait bien être le wiki sémantique : un wiki est un ensemble de connaissance distribué sur un site Web pouvant être édité au moyen du navigateur y donnant accès par une communauté d'utilisateurs et où chaque page dispose d'un historique de modifications. Un wiki

sémantique est un wiki où chaque élément de savoir identifié par un concept (grâce à une ontologie SKOS) est récupérable au moyen du langage de requête SPARQL (Tramp, 2010). Cette possibilité rendrait disponible l'ensemble du savoir de la base de connaissances, quel que soient les tags ou facettes attribués.

- Diffusion

La diffusion (processus n°4 et 5) est traditionnellement répartie en deux modes, l'adressage et la mise à disposition. Un troisième mode hybride est utilisé sur le Web, l'alerte. Utilisant le Really Simple Syndication (RSS), ce mode permet de signaler à un utilisateur ayant choisi de s'abonner au flux la mise en ligne d'un nouveau contenu. Capable d'intégrer une image et une courte description, il permet d'informer le destinataire sur le contenu d'un document sans avoir à envoyer le tout. Le flux peut être basé sur les facettes de la base de connaissances ou sur le suivi d'une expression de besoin particulière. Cependant l'alerte par RSS n'est pas un mode qui a de l'avenir, comme l'indique la fermeture du service Google Reader à l'été 2013. Les technologies futures se basent sur la diffusion/curation communautaire. Plus que par RSS, au sein du Web 2.0 l'alerte vient de collaborateurs (ayant les mêmes centres d'intérêt) au moyen de pages personnelles (Facebook) ou de micro-blogging (Twitter). Bien que l'intégration de lecteur RSS au sein d'intranets et de messageries professionnelles promette de bonnes perspectives d'emploi à ce format d'alerte au sein d'organisations, l'avenir est au microblogging sémantique. A l'image de l'introduction progressive de chat au sein d'intranet, le micro-blogging d'entreprise amènera toutes les capacités de Twitter au sein du cycle de renseignement, notamment : alerte, commentaires, coordination d'activités, assistance, partage d'information (Riemer et al., 2011). Les valeurs ajoutées significatives, avec toute autre forme de diffusion est l'immédiateté et l'interaction. Le contenu d'un document peut être structuré de manière à pouvoir identifier les parties de confidentialité différentes au sein de celui-ci, comme par exemple distinguer ce qui est issu de sources ouvertes et ce qui est issu de capteurs confidentiels, ce qui provient de sources nationales de ce qui provient de partenaires étrangers, alors, grâce à l'extended mark-up language (XML) un document peut être automatiquement diffusé en incluant ou excluant les parties de confidentialité différentes en fonction des destinataires.

2.5. Conclusion

La doctrine française portant sur les opérations civilo-militaires envisage d'utiliser les réseaux sociaux pour développer leurs contacts au sein de la population locale (CICDE, op. cit.,2012). La doctrine portant sur la contre-insurrection annonce comme évolution l'apparition d'une « insurrection connectée » qui en plus d'obtenir par le Web des moyens, C4ISR dispose d'un « *accès aux médias internationaux, aux réseaux sociaux [donnant] une résonance parfois mondiale à leur propagande* » et surtout une opportunité d'agir sur la faiblesse des forces occidentales : leur opinion publique (CICDE, 2013 b).

Avant de pouvoir déployer efficacement des intelligences artificielles au sein de structure de renseignement, il apparait nécessaire de faire évoluer leurs bases de données et leurs méthodologies d'exploitation. Si les bases de données graphes ne sont pas adaptées pour gérer tout type d'expression de besoin, elles permettent un gain de temps considérable dans la capitalisation des données sémantiques. Une structure en Web des cycles de création de renseignement permettra de nombreux raccourcis dans le processus question/réponse du cycle du renseignement. Par exemple la réponse à un besoin en information ne nécessitera pas forcément le re-jeu de l'ensemble des cycles, mais seulement celui de capitalisation (évitant les phases de recueil et d'exploitation). De nombreux freins existent et empêchent le déploiement de technologies telles que les bases orientées graphe. L'urgence affichée par l'État français pour le déploiement de l'intelligence artificielle au sein des structures de renseignement ne doit pas dispenser ces dernières de s'intéresser à l'ensemble des solutions possibles, notamment celles qui proviennent d'années de recherche académique et ce, même en l'absence d'industrialisation. Les systèmes de gestion de bases de données relationnelles ne sont pas la seule technologie possible. Une des directions vers laquelle il peut être intéressant de se tourner sont les bases de données graphes et triples store conçues pour donner du sens à internet au travers du Web sémantique. Afin de prendre en compte cette forte intégration de l'information issue des réseaux sociaux, il est nécessaire pour les structures de renseignement de faire évoluer leurs outils et leurs méthodologies notamment en reprenant ceux employés par les plateformes. Cet appel à une prise en compte et une maîtrise des technologies des Webs initial, social et sémantique dans les cycles de création de renseignement met en évidence la complexité et la richesse de ces Webs pour le renseignement, pas seulement pour améliorer les processus qui le régentent, mais aussi comme source qui l'alimente plus particulièrement dans un contexte de guerre hybride, sujet du chapitre suivant.

3. Chapitre 3. Le renseignement de sources ouvertes dans la guerre hybride

3.1. Introduction

Le renseignement se pense comme une fonction permanente, indépendante du fait qu'un conflit soit en cours ou pas. Cette permanence d'activité se justifie d'autant plus aujourd'hui du fait que certains adversaires mènent une guerre appelée guerre hybride dont les principales caractéristiques que nous commencerons à décrire sont la permanence du conflit et le travail sur la perception des faits et évènements. Impliquant tant civil que militaire, cette forme d'affrontement traduit parfaitement le continuum sécurité-défense ou encore le concept de guerre de mouvements sociaux décrits dans les chapitres précédents. Après en avoir dressé le contour, nous montrerons comment ce principe de guerre aboutit à un nouvel espace de bataille : le théâtre connecté qui amène nos services de renseignement à opérer dans un espace où chaque partie prenante est en mesure de participer à la diffusion, l'interprétation des faits et l'influence sur leur perception. Ce théâtre ne pourrait pas exister sans les médias sociaux. Leur nature même, ce pour quoi ils ont été conçus, et l'usage qu'en font leurs utilisateurs les rendent incontournables qu'elle que soit l'intensité du conflit, de la manifestation à la guerre totale. Nous effectuerons un état de l'art des études à leur sujet en nous concentrant plus particulièrement sur les études portant sur l'interaction de ce Web social avec les mobilisations et contestations d'autorités. Nous étudierons plus précisément les rôles des médias sociaux, présumés et/ou constatés, à travers les conflits auxquels ils ont été mêlés par les différentes parties prenantes de 2006 à 2014. Une fois l'utilisation des médias sociaux caractérisée, nous étudierons leur capacité à fournir des informations sur les évènements auxquels leurs utilisateurs participent du point de vue du renseignement en prenant en compte leur manipulation notamment au travers de systèmes automatisés. Là, se trouve l'ambivalence et la complexité qui réside dans les données issues des médias sociaux, dans la mesure où d'un côté il est possible de les manipuler et de l'autre il n'est pas possible de faire taire tous les émetteurs.

3.2. La guerre hybride et les médias sociaux

La crise ukrainienne a mis sur le devant de la scène le concept de guerre hybride. A titre d'illustration lorsqu'on recherche les nombres de publications sur le thème dans le moteur de recherche Google Scholar on obtient 526 résultats entre 2010 et 2013 et 3640 résultats entre 2014 et 2018. Il existe plusieurs définitions de la guerre hybride, la plupart tiennent compte de l'utilisation par les parties prenantes de moyens non exclusivement militaire afin de prendre l'ascendant dans un conflit. Ces moyens comprennent déploiement rapide et forces spéciales, mesures financières et économiques, cyber opérations défensives et offensives, opérations de renseignement et enquêtes de police, campagnes d'information et usage de médias sociaux. Ce dernier point est probablement ce qui distingue le plus la « guerre hybride » du « conflit asymétrique » ainsi que le rôle particulier donné à la maîtrise de l'information. L'usage de moyen civil pour agir sur un de ses points les plus faibles, sa société, avec pour objet d'amener l'adversaire à se battre sur un terrain où son arsenal militaire ne lui sera d'aucune aide (Major, Mölling, 2015). A ce titre l'information est une arme particulièrement intéressante dans la mesure où : « *elle est bon marché, universelle, dispose d'une portée illimitée, facilement accessible et pénètre toutes les frontières sans restrictions* ». (Darczewska, 2014).

Parmi les opérations d'influence employées on distingue :

- manipulation d'informations, c'est-à-dire l'utilisation d'informations authentiques de manière à donner de fausses implications ;
- fabrication d'informations, c'est-à-dire la création de fausses informations ;
- désinformation, c'est-à-dire la diffusion d'informations manipulées ou fabriquées ou une combinaison de celles-ci.

Dans un conflit hybride, les parties en conflit utilisent les outils médiatiques traditionnels et modernes pour diffuser de nouveaux récits basés sur leurs intérêts, « l'intention principale de la stratégie de subversion politique est d'isoler et d'affaiblir un adversaire en érodant sa légitimité dans de multiples domaines. Les acteurs hybrides saisissent toutes les occasions possibles pour utiliser des instruments médiatiques traditionnels et modernes afin de développer de nouveaux récits basés sur leurs intérêts, leurs moyens et leurs objectifs, « *l'intention principale de la stratégie de subversion politique est d'isoler et d'affaiblir un adversaire en érodant sa légitimité dans de multiples domaines.* » (Jacobs et Lasconjarias, 2015).

La guerre hybride n'est pas un concept nouveau, comme le rappel le Sécrétaire général de l'Otan, Jens Stoltenberg : « *je voudrais souligner que la guerre hybride n'est pas nouvelle. La guerre hybride concerne la combinaison de moyens militaires et non militaires. Il s'agit d'actions secrètes et d'actions manifestes, de tromperie et, en fait, je pense que la première guerre hybride que nous connaissons est le cheval de Troie. Nous l'avons déjà vu, mais la nouveauté, c'est qu'elle se conduit à plus grande échelle, et que cela se déroule près de notre frontière, nous devons donc nous concentrer davantage sur le concept de guerre hybride*. » (OTAN, 2015). Dès 2013, l'actuel chef de l'état-major des forces armées russes et premier ministre adjoint à la Défense, le général Valery Gerasimov, a publié un article projetant les contours du concept russe de guerre hybride mise en œuvre selon trois principes qui se renforcent mutuellement :

- la «permanence du conflit» qui brouille les frontières entre temps de guerre et temps de paix, espace et temps, ainsi qu'entre les acteurs impliqués. En substance, il est de plus en plus difficile de déterminer s'il existe ou non un état de guerre, en particulier pour celui qui est attaqué.
- la «multi-dimensionnalité», la réalisation d'objectifs politiques et stratégiques n'est plus uniquement liée aux moyens militaires conventionnels classiques; le plus important, est la convergence des moyens politiques, économiques, informationnels, humanitaires et autres moyens non militaires qui, à leur tour, permettent d'obtenir les effets stratégiques souhaités, tout en réduisant au minimum la nécessité de déployer une puissance militaire dure.
- l'« effort unifié», c'est-à-dire l'application simultanée de «tactiques mixtes» menées sur l'ensemble du territoire ennemi et, ce qui est plus important encore, au sein de ses «sphères d'influence». La guerre hybride se distingue par la primauté des « opérations d'influence», notamment des communications internes élaborées, des opérations de déception, des opérations psychologiques et des communications stratégiques externes bien définies dans le cyberespace. (Gerasimov, 2013)

Ainsi, en directe application de ces principes la campagne hybride menée par la Russie en Ukraine semble donner les résultats escomptés par Moscou (Thiele, 2015) :

- Déstabiliser un pays en instiguant un conflit interne ;
- Provoquer l'effondrement de l'État en ruinant l'économie et en détruisant les infrastructures ;

- Remplacer les dirigeants politiques locaux par ses propres agents en tant que « sauveurs invités ».

Le concept de guerre hybride n'est pas le pré carré des penseurs militaires. Ainsi les chercheurs en politique du conflit intègrent récemment cette notion, ajoutant une nouvelle forme aux trois types de guerres classiques (interétatiques, extra-étatiques et civiles): les « guerres de mouvements sociaux » contre des États, les deux parties employant des formes de guerre irrégulières (Tarrow et Tilly, 2015). Autre particularité du concept de guerre hybride, elle est quasi systématiquement utilisée par la recherche occidentale pour décrire un moyen employé par l'adversaire (Russie, Chine, Daesh, etc.) alors que de très nombreuses occurrences/ingérences sont relevées à l'encontre des forces occidentales par lesdits adversaires notamment dans leur rôle présumé en tant qu'instigateurs des printemps arabes. En effet, si l'on ne parle pas de manœuvres force est de constater la constance qualification des médias sociaux comme outils de démocratisation, comprendre formatage d'une société sur le modèle occidental, « *les nouvelles formes de communication et les technologies de l'information changent les idées des gens sur la démocratie et les pratiques dans les enceintes publiques.* » (Bijker, Wiebe, 2006). Par exemple le rapport de la Rand Corporation préparé pour le gouvernement américain en 2013 : « Liberté d'internet et espace politique » ne fait pas une seule mention à la guerre hybride, mais conclut que :

- L'expansion de l'espace social en ligne peut entraîner l'expansion de l'espace politique, même lorsque les internautes ne souhaitent pas au départ utiliser Internet à des fins politiques.
- L'information en ligne peut saper le pouvoir autoritaire des régimes non démocratiques en soulignant l'ampleur de l'opposition et en déclenchant une cascade d'informations.
- Internet peut potentiellement rendre les coalitions politiques plus inclusives en ouvrant des possibilités de délibération générant des cadres qui transcendent les clivages socio-économiques.

Ce rapport préconise donc la conception et la mise en place de programmes de libéralisation par internet « Internet Freedom Programs » permettant de : « *élargir l'espace politique, soit en maximisant le nombre d'internautes de base capables de contourner la censure, soit en formant une poignée d'agendeurs - les blogueurs, les journalistes en ligne et les chefs de l'opposition - à devenir des utilisateurs plus sophistiqués de l'anonymisation , du contournement et des technologies de la communication.* » ou encore : « *les programmes pour la liberté d'Internet, qui concernent peut-être uniquement les activités de défense des droits de l'homme des*

gouvernements des États-Unis, visent un large éventail d'activités et de lieux géographiques. Certains programmes, tels que ceux de développement technique, sont de nature globale. Les logiciels publiés sur Internet peuvent être téléchargés ou utilisés par toute personne pouvant y accéder. » (Tkacheva et al., 2013). Cette approche relativement invasive s'illustre notamment au travers de la multitude de projets d'étude de diffusion de masse d'internet menés par des corporations américaines dont certaines ont directement pris part à des conflits sociaux telle que Google dans la révolution égyptienne en permettant aux Égyptiens de contourner le blocage d'internet par le gouvernement pour continuer à diffuser des tweets au moyen d'appel téléphonique gratuit et d'une application appelée speak2tweet (Google, 2011).

Parmi les projets passés et en cours :

- Google avec les projets Loon, des ballons stratosphériques permettant une diffusion équivalente à la 3G (Davies, 2019) ; Titan, des drones de hautes altitudes diffusant l'internet à 1GB/s (Li, 2015)
- Facebook avec le projet Athena, une constellation de satellite permettant de diffuser internet à haut débit qui fait suite au projet de drone Aquila (Olivier, 2018) ;
- Space X, avec le projet Starlink dont les premiers satellites ont été lancé en 2019 (Decourt, 2019).

Il ne s'agit que des projets américains. Il en existe de multiples autres, chinois, russes norvégiens, etc. La diffusion d'Internet depuis l'espace permet de s'affranchir de toutes limites imposées par les États. Depuis l'utilisation des médias sociaux dans les mouvements de démocratisation, de nombreux experts occidentaux s'emploient à renforcer plus encore leur impact dans les sociétés considérées comme dictatoriales. Ainsi les participants au quatrième Symposium annuel Trygve Lie sur les libertés fondamentales Terje Rod-Larsen (diplomate norvégien) se demande : « *comment pouvons-nous travailler pour faire en sorte que les médias sociaux soient utilisés comme un moyen productif, et non contre-productif, pour renforcer la liberté et la démocratie?* » et sa confrère américaine, Maria Otero, sous-secrétaire d'État à la Démocratie et aux Affaires Internationales de renforcer le point : « *comment étendons-nous l'utilisation de cette technologie et des médias sociaux pour qu'ils ne soit pas seulement utilisé pour protester ou exiger, ce qu'il fait si incroyablement bien, mais aussi pour aider à définir les moyens par lesquels les gouvernements sont en mesure de mener leur propre travail en réponse aux besoins de leurs citoyens* » (IPI, 2011).

Ainsi si les gouvernements répressifs peuvent réagir aux soulèvements populaires en recourant à une répression de plus en plus brutale. Dans une large mesure ils ont perdu leur pouvoir sur

le flux d'informations (Loosen et Schmidt, 2012) permettant à des groupes qui ont pu se sentir impuissants face à des régimes répressifs, l'accès à des moyens significatifs grâce au nivellement technologique des médias sociaux sur le terrain politique (Safranek, 2012). Le rôle de la technologie restera intrinsèquement ambivalent et n'est jamais neutre. Même s'il faut : « *éviter le déterminisme technologique ; [et] reconnaître que la plupart des nouvelles caractéristiques des mouvements sociaux résultent de modifications de leur contexte social et politique plutôt que d'innovations techniques en tant que telles.* » (Tilly et Wood, 2012).

Si les opinions divergent encore à ce jour sur l'impact réel des médias sociaux, leur rôle commence à être caractérisé. Ainsi, Tarrow estime qu'internet ouvre de nouvelles opportunités à la condition que les mouvements qui s'en servent aient une vision stratégique et les compétences tactiques nécessaires à une utilisation efficace (Tarrow, 2011). Parmi les rôles des médias sociaux, en plus de la diffusion d'information, on trouve entre autres : l'établissement de l'ordre du jour, l'encadrement des revendications des manifestants (Onuch, 2015), la transformation individuelle en changeant la façon dont les citoyens pensent ou agissent, la polarisation des groupes, la facilitation de l'action collective, et l'attrait de l'attention internationale sur un pays donné. (Aday et al., 2010). Dans le cadre du Printemps Arabe les réseaux sociaux ont permis de proposer : « *de nouvelles formes d'écriture, de critique, de transmission de la mémoire et des informations, d'archivage des évènements dans le but de contributer dans la coordination d'une partie des actions de résistance, de relayer les informations et de couvrir les évènements à travers la diffusion des vidéos amateurs, qui seront retransmises par les grandes chaînes étrangères d'informations* ». (Mihoub, 2011). De plus, les réseaux sociaux : « *se sont offert un espace de rassemblement qui a permis la libération de la parole et la mobilisation politique de la population* » (Soussi, 2011).

Comme chaque média social à son but originel propre, ils ont chacun des atouts spécifiques. Par exemple les recherches indiquent que Twitter a été utilisé pour rechercher des informations, solliciter des dons, organiser des volontaires, publier le nom des personnes disparues et diffuser les besoins immédiats (Starbird, Palen, op. cit.). Pour reprendre les concepts propres à la politique du conflit, les médias sociaux contribuent à la mobilisation, au changement d'échelle du conflit (du niveau local au niveau international), au courtage (intermédiation d'acteurs externes tels que la Russie ou l'Union Européenne dans le cadre de la crise ukrainienne), à la création d'alliances transnationales, la diffusion, la certification, et l'activation des limites (qui sommes-nous ?, qui sont-ils ?).

3.3. Le théâtre d'opération connecté : l'utilisation des médias sociaux de 2006 à 2014

Les médias sociaux numériques font l'objet d'un grand nombre de recherches tant ils offrent un nombre illimité de points de vue sur un nombre illimité de sujets. En rapport avec nos travaux plusieurs thèmes liés à la contestation numérique sont identifiés.

Le concept de mobilisation numérique tel que traité dans les publications francophones est essentiellement associé à la démocratie électronique (Cardon, 2009), et ses variantes thématiques : vote électronique, démocratie participative (Flichy, 2008), démocratie sociale, activité politique sur internet. Internet y est essentiellement décrit comme un moyen et un vecteur d'expression ce qui explique que le thème de mobilisation numérique soit abordé, sans pour autant être le cœur de sujet des ouvrages. Les études portent principalement sur la place de l'individu dans les débats de sociétés notamment les débats politiques lors de campagnes électorales (Benvegnu, 2002), mais aussi lors de débats plus ponctuels autour de thématiques d'actualités comme la défense des sans-papiers, la lutte contre le piratage (Breindl, et Briatte 2009) ou la progression d'idées extrémistes (Duval, 2013). Plus généralement, la mobilisation sur internet est décrite comme une action positive et constructive.

La notion de mobilisation dans le contexte militaire a le sens suivant : « *Mise sur pied de guerre des forces militaires d'un pays par le rappel dans les armées de tous ceux qui sont désignés pour y servir en temps de paix. Ensemble des dispositions prises sur le plan militaire, administratif, économique, etc., pour assurer dans un pays, en cas de menace, la sécurité et l'intégrité du territoire, ainsi que la vie de la population* » (Larousse, 2019) est inexistante dans les publications francophones. Ainsi le rassemblement numérique concerté des forces vives d'une nation ou d'une organisation paramilitaire dans le but de la préparation d'un affrontement n'est pas un sujet d'étude.

Le militantisme numérique et ses dérivés (activisme numérique, hacktivisme, cybercontestation, désobéissance civile numérique) font émerger les concepts de dissidence, d'opposition, de débat citoyen lorsque les autres formes d'expression du débat sont absentes ou réprimées. Deux grands axes de recherche se distingue : les études portant sur les notions de « mouvements sociaux » ou de « société », d'activisme politique en dehors des périodes d'élections (Bargel et Petitfils, 2011 ; Baygert, 2014), ainsi que de grands mouvements

internationaux comme peut l'être le mouvement altermondialiste (George, 2005) ; et les études portant sur la relation entre mobilisation physique et numérique. La première catégorie privilégie les crises et conflit sociaux, mais pas aux conflits armés ou la guerre. Les faits de société, abordés par les publications traitant de sujet tels que le développement des extrémismes, sites racistes, djihadistes (Knobel, 2012), la lutte contre les inégalités (sans-papiers) sont plus clivant (Boussad, 2001) que ceux abordés par la mobilisation numérique. La notion de « démocratie participative » est souvent adoptée dans le contexte révolutionnaire des printemps arabes (Abdallah-Sinno et al. 2013 ; Faris, 2012) ou plus généralement dans un contexte de répression, de régime autoritaire ou de démocratie émergente (Bautès, 2012). Un autre thème est très présent, celui des nouveaux médias par opposition et en lutte contre les médias traditionnels et leur hégémonie sur la diffusion de l'information (Cardon, et Granjon, 2013) ou comme forme de contestation sur une autocensure de ces derniers (Letort, 2014).

A la différence du thème de la mobilisation numérique, celui du militantisme aborde plus fréquemment l'idée de transition du numérique vers le physique démontrant ainsi la capacité d'action d'un mouvement numérique à agir sur l'environnement physique (Manise, 2012). Le militantisme sur l'internet, via l'internet est abordé à la fois comme une extension du militantisme traditionnel et à la fois comme une nouvelle forme d'engagement. Les études portent essentiellement sur des causes justes, ou tout du moins qui s'inscrivent logiquement dans un débat démocratique jusqu'à en pousser les limites dans le cas des mouvements altermondialistes ou les actions d'Anonymous. Les causes extrêmes sont peu étudiées, de même que le lien entre un activisme numérique et activisme physique est rarement évoqué hormis dans le sens du physique (mouvement traditionnel) vers le numérique (extension moderne). Le développement d'un mouvement numérique vers une confrontation physique est parfois abordé dans le contexte des printemps arabes. Cependant la réalité des faits montre que l'activisme de terrain a précédé le militantisme numérique, comme l'immolation de Mohamed Bouazizi a précédé le printemps arabe en Tunisie. Il n'y a pas de texte étudiant la possibilité d'une action concertée de militantisme numérique ayant pour but de constituer une capacité d'action physique sur l'environnement, une capacité de combat au sens militaire du terme.

Le crowdsourcing et autres actions collectives du type « science citoyenne » et le financement participatif « crowdfunding » ne sont pas des thèmes abondement analysés dans les publications francophones. Lorsqu'il l'est, c'est en général dans un contexte économique associé à des concept de création, de bouillon de culture, (Rouzé et al., 2014), de concertation, de collaboration, de co-création marketing (Hamdi-Kidar, 2013), de mobilisation de l'intelligence

collective au sein de projet (Benghozi et Bergadaà, 2012), d'imagination collective à but commercial (Auckenthaler, et al, 2007), voire de nouvelle formes de management, d'organisation du travail (Barlette, 2013).

A ce jour, il n'existe pas d'étude sur les outils mis à disposition des utilisateurs du Web permettant la mise en commun de leurs compétences et sur la façon dont ces outils démultiplient leurs capacités dans un conflit. Il n'est fait mention nulle part d'associer la puissance de la foule à une cause politique, à une action militante ou militaire dans le cadre d'un effort concerté en avance de phase de manifestations.

Enfin abordons les déclinaisons physiques de mobilisation numérique qu'il s'agisse de flashmob[1], mouvements sociaux (protestation organisée), activisme (militantisme : recrutement/rassemblement), théories de l'action collective, comme expliqué précédemment, il existe peu d'étude sur les liens entre action physique et action numérique ou sur les déclinaisons physiques de rassemblement numérique. Le seul effet qui est abordé est sans-doute le plus éphémère et ayant le moins d'impact par définition : la mobilisation éclair ou flashmob. Ce phénomène récent (2003) est rarement le sujet central d'études francophones. Il est souvent abordé en association avec des thèmes comme la mobilisation à travers les réseaux sociaux ou les nouveaux usages liés aux nouvelles technologies de l'information et de la communication. Deux types de flashmobs se distinguent, celles génératrices de « buzz » à but commercial, celles d'apparence gratuite sans objectifs déclarés. Malgré cet aspect futile et cet effet temporaire, ces flashmobs sont le fruit d'une organisation et d'une coordination qui sont loin d'être anodines quand bien même le but recherché ne serait que ludique ou commercial. L'étude de la méthode pour organiser efficacement une flashmob ou tout autre extension physique d'un mouvement numérique est absent des écrits francophones. Pourtant le cas récent du mouvement de contestation : « la manif pour tous » est un exemple de cette volonté de coordination d'un mouvement numérique et physique à des fins politiques.

La guerre sur internet est l'objet de très nombreuses études en fonction du point de vue choisi. Il est souvent question de cybersécurité, de guerre de l'information, de cyberterrorisme; cybercriminalité, de cybermercenariat lorsque celui-ci ne poursuit qu'un but commercial ou criminel ou de toute forme d'utilisation d'internet par les forces armées autre que pour le combat (ex : relations publiques). Le thème de la cyberguerre est très bien représenté dans la recherche francophone. Cependant il génère une très large confusion de sens comme le confirme l'Officier

[1] Fusion des mots flash et mobilisation, il s'agit d'un rassemblement public d'un groupe de personnes pour effectuer une action coordonnée avant de se disperser rapidement.

Général à la Cyberdéfense, le vice-amiral Coustilliere : « *En France, on a tendance à confondre la cyberguerre et la cybercontestation* » (Regard sur le numérique, 2015). De nombreux articles mélangent des concepts fondamentalement différents tels que cyberguerre, guerre de l'information, cyberterrorisme, cybersécurité, cyberdéfense, etc. (Yagil, 2002). Les études faites sur le sujet de la cyberguerre sont en général d'un niveau stratégique et géopolitique et abordent des sujets comme l'éventualité d'une cyberguerre (Garrigue et Kempf, 2012) ou se demandent si elle a déjà lieu. Il arrive que le niveau opérationnel soit abordé, et plus rarement le niveau tactique. Dans ce dernier cas seuls les enquêtes post-attaques sont étudiées. Plusieurs points spécifiques sont observés tels que les aspects géographiques (Mongin, 2012) pour en délimiter les espaces (Ventre, 2010), ses aspects juridiques (Schmitt, 2002) ou encore pour détailler des domaines spécifiques tels que les attaques, les défenses (Ventre, 2011) et les méthodes d'enquêtes (Thonnard, 2010). D'autres recherches encore constituent un retour d'expérience sur un conflit spécifique comme la Syrie (Pellet et al., 2014). Le point commun à toutes ces études est de mettre en évidence la complexité et la haute technicité requise pour combattre sur internet. Les attaques seraient le fait d'experts et la défense nécessiterait des ingénieurs de haut niveau (Turse, 2012). Sans nier cette réalité, le fait est que, chaque jour, les outils mis à disposition par l'internet deviennent plus simples pour des effets toujours plus puissants, réduisant ainsi le socle de connaissances nécessaires à leur utilisation et par extension rendant leur emploi par la foule possible. Aucune étude ne décrit les outils mis à disposition du grand public permettant de remplir une ou plusieurs fonctions C4ISTAR pour une maîtrise opérationnelle et tactique par un groupe de son théâtre d'opération bien que de nombreux exemples partiels existent tels que la coordination des zadistes à Nantes en 2014, ou des émeutiers lors des émeutes de Paris en 2005.

Comme nous le verrons ci-après le lien entre médias sociaux et conflits est réel. Sans préjugé d'un éventuel rôle spécifique, dans un premier temps nous effectuerons un constat des liens entre mouvement social et médias sociaux. Si parmi ces conflits, ceux qui ont été les plus étudiés sont ceux dit des « Printemps Arabes », chaque contestation qui les a précédés ou suivis a apporté sa contribution à l'utilisation des médias sociaux pour la contestation. Rapidement nommés les « Révolutions Twitter » par les médias traditionnels, la plupart des études à leur sujet ont démontré que les médias sociaux avaient effectivement joué un rôle déterminant. Cependant ils n'ont jamais été nommé comme la cause principale ou le point de départ de ces révolutions. Au mieux on se borne à constater que certains changements d'algorithmes ont pu permettre à certain mouvement de connaître un engouement initial qu'il n'aurait pas eu sans l'internet comme pour les gilets jaunes par exemple (Broderick et Darmanin, 2018). Chacun de

ces conflits a pu bénéficier à la fois de la progression constante de la technologie mise à disposition par les médias sociaux et de l'augmentation exponentielle de la base d'utilisateurs actifs. En fait, et ce sera en partie l'objet de notre recherche, malgré les zones géographiques distinctes, les causes sous-jacentes variées, il est permis de penser que les expériences d'utilisation des médias sociaux dans ces conflits ont pu bénéficier aux contestataires successifs, comme un répertoire d'actions collectives globales.

En 2012, Safranek établit la liste suivante comme les premières crises au cours desquelles les médias sociaux ont joué un rôle significatif : Moldavie 2009, Iran 2009, Tunisie 2010, Egypte 2011, Syrie 2011, Azerbaïdjan 2012 (Safranek, op.cit.). Dans nos travaux nous ajoutons à cette liste la crise ukrainienne de 2014.

Le conflit en Moldavie (été 2009) n'est sans doute pas le premier cas d'utilisation des médias sociaux dans le contexte d'une contestation. Les outils avaient atteint un taux de pénétration suffisant pour que leur utilisation soit remarquable. De plus, il s'agit d'un des premiers à avoir été étudié par la communauté scientifique (Shirky, 2011). Dans le cadre d'élections parlementaires contestées, leurs conclusions mettent en évidence l'utilisation privilégiée des médias sociaux par les manifestants pour coordonner leurs rassemblements via Facebook et LiveJournal (Shirky, ibid.).

La tentative de révolution en Iran en 2009 est un autre cas particulier. Il s'agit de l'un des premiers conflits sociaux où les médias sociaux ont été utilisés au maximum de leur efficacité à la fois par les contestataires, mais également par les forces de l'ordre à des fins répressives lors des manifestations faisant suite aux élections présidentielles de 2009. Preuve de l'importance de ce réseau social pendant le conflit, le gouvernement américain a même demandé à Twitter de retarder une mise à jour qui aurait pu couper l'accès à la plateforme en journée pour les manifestants (Pleming, 2009). « *Une mise à niveau critique du réseau doit être effectuée pour assurer le fonctionnement continu de Twitter. En coordination avec Twitter, notre hôte réseau avait prévu cette mise à jour pour ce soir. Cependant, nos partenaires du réseau NTT America reconnaissent le rôle que Twitter joue actuellement comme un outil de communication important en Iran. La maintenance planifiée de ce soir a été reprogrammée à demain entre 2 et 3 heures PST (1:30a en Iran).* » (Twitter, 2009). La plateforme Twitter a été massivement utilisée, au point où, pour la première fois depuis l'utilisation systématique des médias sociaux en période de conflit, la contestation a reçu l'appellation de « Révolution Twitter » (Tusa, 2013). Deux réserves doivent être apportée à cette qualification. Tout d'abord le nombre réel d'utilisateurs actifs de Twitter effectivement en Iran lors des manifestations est

estimé à quelques centaines d'individus comparé aux centaines de milliers de manifestants. De plus le gouvernement a également utilisé twitter pour organiser des contre manifestations et leurrer des opposants vers des faux rassemblements, diffuser des rumeurs et des messages pro-régime (Aday et al, op. cit.,2010).

La révolution tunisienne en 2011 est la deuxième révolution (après l'Iran) ayant reçu l'appellation de « Révolution Twitter ». Si les médias sociaux ont été massivement utilisé lors de cet événement, ils ont eu un rôle de catalyseur : « *Ils ont accéléré les réactions sociales locales, synchronisé les différents niveaux et intensités des soulèvements et permis une couverture des évènements auprès de l'opinion publique globale en temps-réel.* », (Benkirane, 2012). Les mêmes activités vues lors des conflits sociaux précédents apparaissent en Tunisie : communication, coordination, cadrage, témoignage, etc. De nouveau, face à un régime autoritaire maîtrisant totalement les médias traditionnels, les médias sociaux : « *éliminent les portiers ayant pour conséquence que l'information n'est plus exclusivement diffusée de quelques diffuseurs vers la masse mais de la masse vers la masse.* » (Lamer, 2012.)

Lors de la révolution égyptienne, qui dans la mode médiatique des Printemps Arabes reçu également le qualificatif de Révolution 2.0, comme le tweete un manifestant : « *Nous utilisons Facebook pour organiser nos manifestations, Twitter pour nous coordonner, et Youtube pour diffuser vers le monde entier* » (Rashed, 2011). En plus des activités de l'ensemble des protagonistes observées sur les médias sociaux dans les conflits précédemment cités, un nouveau type d'affrontement est apparu. Deux jours après le début de l'affrontement, le gouvernement tenta de couper l'accès à Internet. Parmi les multiples méthodes de contournement trouvées localement, un acteur extérieur et non des moindres, apporta une contribution significative : Google en partenariat avec Twitter et SayNow mit en place un dispositif d'émission de tweet (conversion texte-voix, hashtag #egypt automatique) directement à travers des numéros de téléphones gratuits (Google, 2011). Ainsi une corporation privée décide de son propre chef d'intervenir dans un conflit social étranger, elle réitérera son opération un peu moins de deux années plus tard en Syrie (Google, 2012). Au vu de l'inefficacité de la coupure et du fort impact négatif (économiquement et médiatiquement) le gouvernement remit en place l'accès à Internet cinq jours après l'avoir coupé.

Au moment de la révolution syrienne, l'utilisation des médias sociaux à toutes les étapes (mobilisation, coalition, confrontation) est constante. Et comme dans les cas précédents, elle a apporté sa part d'innovation. Ainsi, malgré la violence des combats en Syrie, même dans les villes réduites à l'état de ruines sous le contrôle de groupes de terroristes, après cinq ans de

guerre civile (en 2016), les rebelles avaient toujours accès à Internet. Une enquête du journal allemand Spiegel (Kwasniewski, 2015) démontre les techniques utilisées pour bénéficier de l'accès par satellite à Internet, permettant un « *taux descendant de 22 Mégabits secondes et un lien ascendant jusqu'à 6 Mégabits* ». À titre de comparaison, les vitesses moyennes dans les villes d'Europe occidentale sont de 2 à 8 mégabits et jusqu'à 1 mégabit. Les liaisons par satellite mises en place localement permettent la diffusion de réseaux via des répéteurs Wi-Fi donnant accès au plus grand nombre permettant à tous les protagonistes de mener leur combat en ligne. Un autre développement majeur provoqué par le conflit syrien est qu'une organisation terroriste, Daesh, a démontré sa maîtrise absolue des médias sociaux : « Leur utilisation agressive des technologies modernes de l'information, de la communication et du renseignement a accru l'efficacité de leur activité » (Stern et Berger, 2015). Daesh contrôlera jusqu'à 90 000 comptes Twitter, ce qui ajouterait jusqu'à 10 000 comptes en une seule opération (Gladstone, 2015).

Dans les premiers moments du mouvement social en Azerbaïdjan, où la contestation reste maîtrisée par les autorités, les médias sociaux sont utilisés quotidiennement par l'opposition pour organiser des événements, collecter des fonds, et inversement par le gouvernement pour la surveillance d'activistes, les campagnes pro-gouvernementales et l'action directe (Pearce 2014b). D'ailleurs ce qui distingue ce pays des autres est l'utilisation active des autorités pour dénigrer et délégitimer toute forme d'opposition au travers des médias sociaux. Pearce démontre comment les autorités ont fait évoluer leur utilisation des médias sociaux avec le développement de ceux-ci passant d'une posture défensive jusqu'en 2009 où les citoyens étaient libres de s'exprimer alors que les autorités se servaient des contenus diffusés pour mener leur répression, à une posture offensive où les partisans pro-gouvernementaux utilisent de nombreuses techniques de saturations pour occuper l'espace des médias-sociaux avec leurs contenus allant de fausses-informations à compromissions de figures de l'opposition (Pearce, 2015).

Lors de la crise ukrainienne de 2014, les différentes parties prenantes ont très largement utilisé les médias sociaux. Qu'il s'agisse de médias occidentaux (Facebook, Twitter) ou russes (Vkontakte, Odnoklasniki), des masses d'informations et de désinformations ont été diffusées. La deuxième partie de notre recherche est consacrée à la description de la crise au travers du prisme des réseaux sociaux, de Twitter en particulier. Leur étude, basée sur notre expérience du terrain (voir annexe 1) est l'objet de la seconde partie de nos travaux.

Bien que les multiples possibilités de communication et de documentation offertes par les médias sociaux en temps de révolution soient claires, le rôle de déclencheur attribué aux médias sociaux par les médias traditionnels occidentaux depuis les manifestations de 2009 en Iran et plus particulièrement depuis le Printemps Arabe est discuté. Sur le sujet de leur rôle, le United States Institute for Peace dans son rapport « Blogs and Bullets II » établit que les médias sociaux ont eu un rôle de diffusion de contenu ayant pour effet la mise à disposition de témoignages et non un rôle d'instigation des révolutions en Tunisie, Égypte, Libye, et au Bahrain (Aday, 2012), David M. Faris appelle à dépasser le concept de révolution par les médias sociaux pour considérer la révolte en réseau comme nouveau facteur à prendre un compte dans les révolutions : « *La révolte en réseau n'est pas un phénomène mono-causal - les médias sociaux ne sont pas seuls responsables de l'action collective, ils n'influencent pas non plus d'une telle manière.* » (Faris, 2012). En outre, la nature et la portée de l'impact immédiat et à long terme des médias sociaux n'ont pas encore été quantifié. Si certains considèrent les médias sociaux comme un outil de démocratisation (Diaz-Ortiz, Stone, 2011), en particulier dans les pays autoritaires, d'autres estiment que ces outils, utilisés par toutes les parties prenantes, favorisent les oppresseurs (Gunitsky, 2015).

Il a été établi que les médias sociaux jouent un rôle actif dans les interactions sociales, en particulier en période de conflit, mais leur utilisation et leur rôle spécifiques sont sujets à discussion par les experts. Il est très difficile pour les experts de prouver leurs conclusions, que leur travail ne puisse pas être reproduit dans différents ensembles de données ou en raison de contraintes de propriété des propriétaires de données. Afin de rendre les résultats plus duplicables, nous croyons en une approche uniforme visant à fournir un protocole standard de préparation des données et des grilles d'observation afin de permettre aux ensembles de données de médias sociaux de parler d'eux-mêmes en période de conflit avant leur analyse et la conclusion qui en découlera.

Au-delà de leur rôle supposé ou avéré en termes de facteurs essentiels ou déclencheur de la contestation sociale ne peut être tranché, il est malgré tout tangible. Les médias sociaux contribuent quotidiennement à une meilleure interaction entre un individu et son environnement informationnel, entre un individu et son environnement physique, entre les individus entre eux en temps de paix comme en temps de guerre. Nos recherches indiquent qu'au minimum, les médias sociaux fournissent une image réaliste de l'événement en cours, à la manière d'un radar ou d'un sonar décrivant leurs cibles. Il peut comporter des biais et des limitations, mais indiquer clairement la nature, la position, le rythme et le cap.

3.4. Information et renseignement sur les réseaux sociaux : création, diffusion, et influence

Dans la continuité de l'histoire des médias, l'internet se transforme en cumulant des évolutions, est une ressource, une nouvelle génération arrive sans remplacer ni modifier le contenu de la précédente. La génération prise en considération dans cette recherche, le Web social, provient du Web initial composé essentiellement de documents numériques reliés entre eux par des liens hypertextes. Cette deuxième génération de Web, dit social ou 2.0 offre de nouveaux moyens aux utilisateurs en leur permettant d'avoir une plus grande interaction avec leur environnement informationnel, une plus grande maîtrise de l'information.

Il existe sur internet près d'1 milliards 700 millions de sites Web en ligne dont seulement 200 millions actifs (Internet Live Stats, 2019). Parmi les six sites les plus visités chaque jour, trois sont des réseaux sociaux : Facebook, Instagram, Twitter (Similar Web, 2019). Les médias sociaux sont une façon de nommer un ensemble d'outils de communication disponibles sur le Web. Ces outils sont considérés comme « médias » dans le sens où ils permettent la diffusion de contenu et « sociaux » car ils reposent sur une infrastructure de réseau social numérique.

Simples d'utilisation, en développement constant, ils mettent à la disposition de tout individu connecté un large faisceau de possibilités pour exprimer une opinion. Ils peuvent être catégorisés de plusieurs manières : par la nature des données diffusées (texte, image, vidéo, audio, etc.) par le but de diffusion (partage, commentaire, alerte, visualisation, collaboration, etc.) ou bien encore par le type de communauté affiliée. Si les opinions et les études divergent sur les définition et catégorisation des médias sociaux, tous s'accordent à leur reconnaître un rôle majeur dans les relations humaines aujourd'hui. Leur succès se mesure aux nombres de personnes les utilisant activement. En 2018, environ 2,65 milliards de personnes utilisaient les médias sociaux dans le monde, ce nombre devrait atteindre près de 3,1 milliards en 2021(Statista, 2019a ; 2019b).

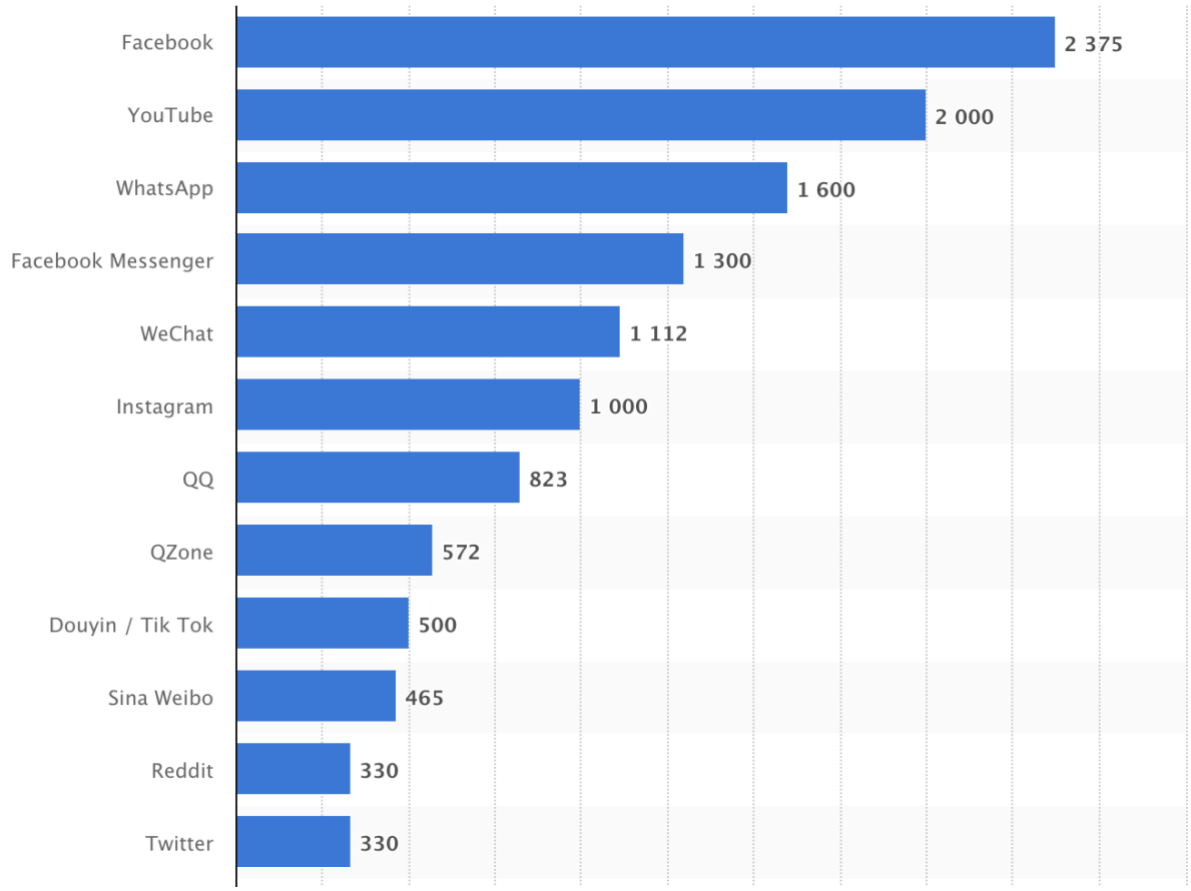


Figure 3 : Plateformes de médias sociaux en millions d'utilisateur actifs mensuels (Statista, 2019b)

Chacune de ces plateformes rentre dans plusieurs catégories, et si elles ont un contenu et une vocation spécifiques à leur création, dans les faits elles permettent toutes de créer, diffuser, commenter des données numériques avec une grande interaction sociale. Chaque utilisateur devient une source potentielle d'information pour le renseignement de sources ouvertes, un capteur en mesure de témoigner d'évènements en cours. La façon de classer les médias sociaux proposée par Cosenza est indépendante du contenu diffusé. Elle résulte d'un croisement entre leur propriété temporelle (éphémère ou permanent) et la nature des destinataires (audience restreinte ou mondiale). (Cosenza, 2012).

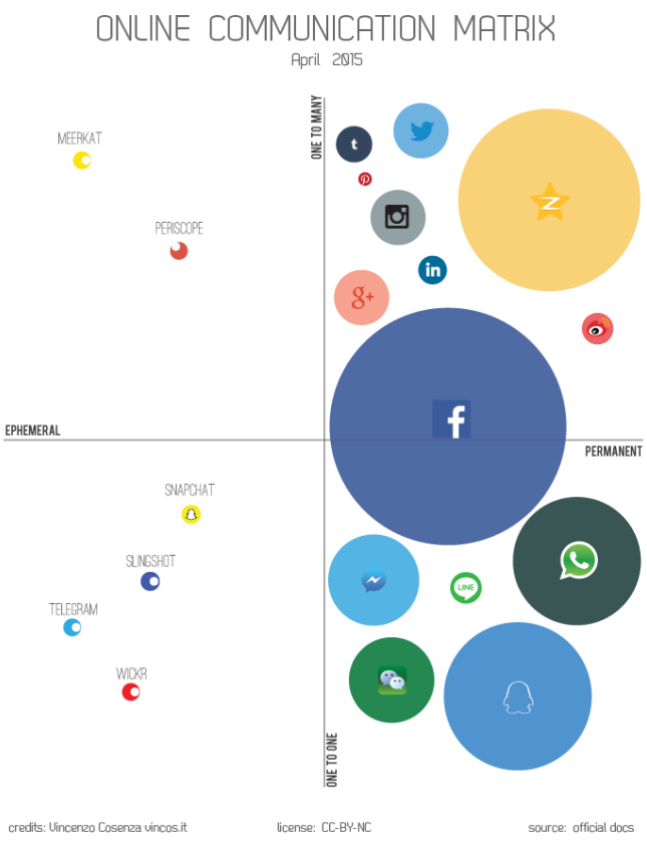


Figure 3b : Classement des médias sociaux par utilisation (Cosenza, 2012)

Ce classement, voire figure 3b, permet de mettre en évidence le fait que la très grande majorité des médias sociaux laissent leur contenu accessible de façon permanente et que leurs contenus se destinent autant à une diffusion publique que restreinte. Une étude du Global Web index montre que les utilisateurs des médias sociaux ont en moyenne 8 comptes sur des réseaux sociaux et sont actifs sur près de la moitié de ces comptes, ce qui permet de penser qu'un utilisateur aura un compte pour la diffusion de contenu public et un autre pour diffuser du contenu privé (Global Web Index, 2018). En matière de diffusion de contenu, ces plateformes mettent continuellement de nouvelles capacités, de plus en plus performantes, aux mains de tous leurs utilisateurs comme l'indique Mark Zuckerberg le dirigeant de Facebook : « *À tout moment donné, il n'y a pas qu'une seule version de Facebook qui fonctionne, il y en a probablement 10 000. N'importe quel ingénieur de l'entreprise peut décider qu'il veut tester quelque chose. Il y a des règles sur les choses sensibles, mais en général, un ingénieur peut tester quelque chose, et il peut lancer une version de Facebook non pas à l'ensemble de la communauté, mais peut-être à 10 000 ou 50 000 personnes – soit le volume nécessaire pour faire le bon test d'une expérience* » (Huspeni, 2017).

Cet effort constant de simplification, de vulgarisation de la haute technologie du Web intégrée et son intégration systématique dans les versions mobiles des plateformes change complètement la façon dont les utilisateurs interagissent avec leur environnement informationnel. De simples consommateurs, ils deviennent acteurs à part entière et en temps réel de cet environnement. Cette action s'inscrit dans un contexte collectif. Si un utilisateur peut utiliser un réseau social à titre individuel il s'agit d'un phénomène assez rare, la tendance étant aux petites ou grandes communautés au sein d'un réseau global (Kumar, et al., 2006).

Cette évolution majeure implique plusieurs changements importants dans la vie quotidienne, dans toutes les interactions sociales, y compris pendant les périodes de forte tension. Depuis 2010/2011, période où des plates-formes comme Facebook qui atteignirent plus de 500 millions d'utilisateurs ou encore 200 millions pour Twitter, aucun événement social n'a plus eu lieu sans avoir été commenté. Même une opération des plus secrètes telle que le raid contre Oussama Ben Laden au Pakistan par les forces spéciales américaines a été tweetée en direct par l'utilisateur de Twitter @ ReallyVirtual (Sohaib, 2011).

Le succès des médias sociaux répond au modèle d'acceptation de la technologie adapté de Davis (1986). Les critères standards sont : la perception de l'utilité, la facilité d'utilisation, l'attitude de l'utilisateur envers la technologie, l'intention d'utiliser la technologie, l'utilisation effective de la technologie, auxquels s'ajoutent la taille critique, l'aspect ludique, et la fiabilité (Rauniar et al., 2014). Ces trois derniers critères expliquent comment un média social gagne en popularité parmi une catégorie d'utilisateurs et surtout comment sa masse critique et sa fiabilité s'auto-entretiennent.

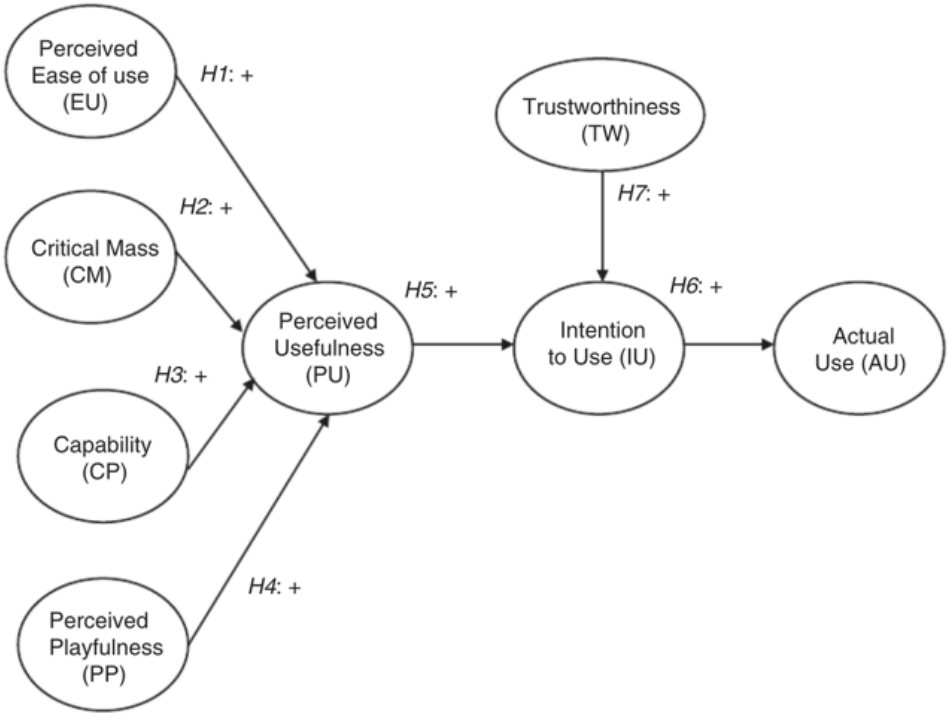


Figure 4 : Technology acceptance model and social media usage (Rauniar, et al., 2014)

Parmi les principales raisons invoquées par les utilisateurs pour expliquer leur présence sur les médias sociaux on trouve : rester en contact avec des proches, se maintenir informé, partager ses opinions, des photos et des vidéos (globalWebindex.com/chart-of-the-day/social-media, 2018).

Le fait qu'il n'y ait pas de limites au nombre de balises sur un document permet à l'utilisateur de les utiliser en deux sens. Le premier, en tant qu'auteur grâce à des balises suggestives, métadescripteurs de sa perception du contenu. Il catalogue les contenus avec ses propres termes pour mieux les retrouver, les associer, comme le fait un tweetos avec des hashtags. Le second, qui s'inscrit dans le cadre collectif du réseau, est le balisage de contenu par l'utilisateur et répond au besoin de partager un document et d'exprimer un jugement sur la nature et/ou la valeur de son contenu. Cette expression personnelle à l'attention de la communauté est une véritable nouveauté et une plus-value portée par les réseaux sociaux.

Ces deux utilisations du balisage social sont rendues plus complexes par l'augmentation du nombre de documents et le développement de la communauté. Ainsi, plus il existe de documents balisés subjectivement « à lire », ou encore, plus de gens marquent des documents comme portant sur un sujet spécifique, moins le tag a du sens (Furnas et al, 2006).

Plus un tag est populaire moins il caractérise un document en particulier, perdant ainsi de son intérêt en tant que descripteur de contenu (Chi et Mytkowicz, 2008). Dans un article précédent, ces auteurs décrivent un phénomène d'entropie qui incite les utilisateurs à réemployer les mêmes tags utilisés dans leur communauté créant de fait une sorte de vocabulaire contrôlé (Chi et Mytkowicz, 2007). Cette restriction dans l'utilité des tags est compensée par l'augmentation du nombre de tags par document. Ce n'est plus un tag, mais une combinaison spécifique de tags qui décrivent le contenu.

Trois autres limitations sont décrites par Golder et Huberman : la polysémie, la synonymie, et « la variation du niveau de base » (Golder et Huberman, 2005). La polysémie est facteur de bruit et entraîne la découverte de documents n'ayant rien à voir avec la recherche initiale. La synonymie est cause de silence, car l'utilisateur ne connaît pas tous les tags qui peuvent être employés pour décrire un document. « La variation du niveau de base » est l'expression de la difficulté à déterminer quel niveau de précision doit avoir un tag (par exemple « Windows » est balisé comme système d'exploitation, un logiciel, un produit de Microsoft, etc.). Ces trois limitations qui existent dans tout système de recherche de contenu sont compensées par les moteurs de recherche au moyen d'une indexation complète du texte et par les autorités classificatrices à l'aide de l'imposition d'un vocabulaire contrôlé.

De prime abord paradoxal, le développement de la communauté d'utilisateurs, qui est présenté comme une limitation à l'intérêt du balisage social, est potentiellement une solution pour en conserver la pertinence. De nombreuses études font état de l'émergence d'une forme structurée, au niveau global du réseau qui englobe les communautés d'un site, appelée folksonomie (Au Yeung et al., 2008). Ce terme inventé par Thomas Vander Wal (Vander Wal, 2007) identifie l'émergence de « […] *schémas de classification construits socialement (sans apport d'un architecte de l'information)* […] » (Smith, 2008). L'idée défendue est qu'une classification du bas vers le haut, de l'utilisateur vers la plateforme, émerge de l'ensemble des balises de contenus (tags) attribuées au corpus de documents. Cette classification s'oppose à celle des annuaires et autres formes classiques de catégorisation où la structure du haut vers le bas impose avec beaucoup de rigidité un ensemble déterminé de catégories initiales, un vocabulaire contrôlé, voire un thésaurus et une ontologie. Le terme de classification est excessif, il y a en effet plusieurs schémas qui se dégagent de l'ensemble des tags attribués à un document. Golder et Huberman remarquent, dans le corpus de tags attribués par une communauté d'utilisateurs, la distribution caractéristique des lois de puissance, un petit nombre de tags très fréquemment utilisés suivi d'une longue traîne de nombreux tags faiblement utilisés (Quintarelli, 2005). Cette

distribution explique tout l'intérêt du balisage social dans la mesure où, tout en exprimant un consensus dans l'utilisation de quelques tags représentatifs de la perception d'un document au sein de la communauté, il préserve la possibilité de décrire le contenu d'un document de façon personnelle. Ils ajoutent qu'« *après un nombre relativement faible de tags, un consensus naissant semble se former, un consensus qui n'est pas affecté par l'ajout de nouveaux tags* ». Cette stabilité est la conséquence d'un effet « d'imitation et de savoir partagé. » (Golder et Huberman, 2006).

Ces tendances stables dans la description, signe d'une intelligence collective font la force des réseaux sociaux numériques.

Les médias sociaux, de par leur nature même, provoquent une perte de contrôle centralisé de l'information par les médias traditionnels, qu'ils soient contrôlés par des organismes publics ou privés. Cette perte de contrôle peut être une condition de conflictualité, car « *les personnes qui sont prises dans une crise utilisent leur téléphone portable et autres dispositifs de communication pour faire connaître les conditions locales au travers d'une plate-forme d'agrégation* » (Livingston et Walter-Drop, 2012). Cela peut être bénéfique, dans la mesure où il renforce la société civile en accroissant la participation des citoyens grâce à la collecte, au partage et à la formulation d'informations de manière autonome. Ce renforcement a été particulièrement visible lors des crises sociales des cinq dernières années.

Compte tenu de leur utilisation par des masses de personnes, dépassant en volume toute forme de système de sondage et d'interrogation sociale, les médias sociaux apparaissent comme un support d'étude sociologique idéal. Danah Boyd fait référence à 671 études menées entre 2002 et 2015 sur des réseaux sociaux, dont 268 sur des micro-blogs en particulier sur Twitter entre 2007 et 2015 (Boyd, 2015).

Les examens journalistiques, universitaires et populaires du rôle spécifique des médias sociaux ont abouti à des conclusions contradictoires, qui peuvent poser des problèmes pour mesurer l'impact des interactions sur les médias sociaux. Reflètent-ils avec précision les mouvements et les réactions sociales en temps réel ? Il existe quelques études sur les limites de la recherche sur les médias sociaux. L'une des limites est le problème de la représentativité, qui se situe à deux niveaux (Cihon Yasseri, 2016) : celle de la représentativité des utilisateurs de médias sociaux par rapport à la population en général et celle des données collectées par rapport à toutes les données disponibles sur un sujet.

Sur le premier point, chaque média social a une population type (classe d'âge, sexe, catégorie socioprofessionnelle) et est le véhicule d'un contenu typique (actualités, photo, vidéo, etc.) qui

influence largement la nature des recherches effectuées sur ce support. "Instagram, par exemple, a un attrait particulier pour les adultes de 18 à 29 ans, les Afro-Américains, les Latinos, les femmes et les citadins, tandis que Pinterest est dominé par les femmes de 25 à 34 ans au revenu moyen de 100 000 $" (Ruths et Pfeffer, 2014). Ce point sert souvent d'argument aux commentateurs qui nient la valeur des médias sociaux pour les études sociales par rapport aux approches qualitatives traditionnelles. Nous pensons que bien que cette limitation soit réelle et significative, elle ne s'applique pas à tous les types d'études sociales. En outre, comme il sera présenté dans le présent document, en matière d'analyse des troubles sociaux, les médias sociaux offrent, comme aucun autre média, des capacités essentielles aux chercheurs, indépendamment de la représentativité sociale.

Sur le second point, les limites des collections gratuites via des API[2] de médias sociaux propriétaires ne sont ni explicites ni stables : « *il est impossible de savoir à quel point l'ensemble de données est complet* » (Burgess, Bruns, 2012). Une collection constituée par une équipe de recherche peut être radicalement différente de celle d'une autre sur un sujet similaire. De plus, il est souvent interdit par les accords d'utilisateur final et les conditions de vente de partager des données achetées, ne serait-ce que pour valider les résultats, selon la méthode de « peer review » à la base de toute publication scientifique importante (Ruths et Pfeffer, op. Cit.). Ceci est la source de restriction la plus importante, uniquement imposée par les plates-formes de médias sociaux pour des raisons économiques et éthiques et non pour des raisons de capacités techniques. Il appelle clairement à un accès ouvert à des ensembles de données pseudonymisées en masse grâce à des partenariats avec des instituts de recherche.

Compte tenu des taux (en croissance constante) de pénétration de l'internet (Internet World Stats, 2019), de progression de l'urbanisation (World Bank, 2019), d'utilisateurs actifs des médias sociaux (Statista, 2019b), il est évident qu'ils sont désormais un élément incontournable de la communication moderne. Malgré des questions encore ouvertes sur le rôle des médias sociaux dans une société, leur impact potentiel sur l'opinion publique en fait un vecteur de diffusion de masse particulièrement puissant. Une tentative d'influence se caractérise par la volonté d'un groupe, d'un gouvernement ou de n'importe quelle organisation d'influencer le cours d'un ou des événements afin d'obtenir ou de tendre vers un objectif précis.

[2] L'interface de programmation d'application (API) permet à différents logiciels d'interagir entre eux. Cela permet par exemple a un logiciel de collecte et de mise en base de données de se connecter directement aux bases de données de Twitter.

Au deuxième trimestre 2018, Twitter comptait 335 millions d'utilisateurs actifs par mois. Cependant selon une étude récente, jusqu'à 15% d'entre eux seraient des bots (Varol et al., 2017). Ce phénomène caractérise un second travers des médias sociaux. Parce qu'étant totalement numériques, ils paraissent plus facilement manipulables dans un contexte de guerre hybride. Une enquête du New York Times répartit les bots en 3 catégories :

- les bots programmés publient des messages en fonction de l'heure ;
- les bots d'observation surveillent d'autres comptes Twitter ou sites Web et tweetent lorsque quelque chose change ;
- les bots d'amplification suivent, retweet et aiment les tweets envoyés par des clients ayant acheté leurs services. (Confessor et al., 2018).

Heureusement, ces bots sont guidés par des algorithmes, ils sont donc détectables par d'autres algorithmes. Les manipulations les plus complexes restent l'œuvre d'humain notamment au travers de « fermes à trolls » sur les médias sociaux. Le groupe européen d'experts de haut niveau sur la désinformation en ligne définit la manipulation comme étant : « *toutes les formes d'informations fausses, inexactes ou trompeuses conçues, présentées et promues pour causer intentionnellement un préjudice à la population ou à des fins lucratives.* » (Commission Européenne, 2018). Dans leur rapport conjoint, le Centre d'analyse, de prévision et de stratégie et l'Institut de recherche stratégique de l'École militaire inscrivent la manipulation au sein des manœuvres traditionnelles telles qu'influence, propagande, et désinformation, auxquelles s'ajoutent les formes modernes fake news, et autres post-vérités (CAPS, IRSEM, 2018). Ce rapport définit deux catégories d'auteurs de désinformations, les acteurs non étatiques tels que les groupes djihadistes, les communautés ethniques et/ou religieuses, les mouvements nationalistes et/ou populistes ; et les acteurs étatiques qui agissent sur leur propre population ou sur celle de leurs adversaires. Le cas de la Russie est particulièrement détaillé dans ce rapport dans la mesure où son intervention dans la crise ukrainienne de 2014 est devenue un modèle de guerre hybride utilisant tout autant l'espace géographique que l'espace numérique, pour agir tant sur les corps que sur les esprits, avec un objectif nouveau : « *Il s'agit moins de convaincre que d'affaiblir en divisant.* ».

Si les médias sociaux semblent particulièrement exposés à ces opérations ils disposent intrasèquement du germe de leur salut, l'approche multidimensionnelle prônée par l'Union Européenne en est une illustration. En effet, pour lutter contre la désinformation, parmi les mesures préconisées deux sont renforcées par les médias sociaux :

- *développer des outils permettant aux utilisateurs et aux journalistes de lutter contre la désinformation et de favoriser un engagement positif vis-à-vis des technologies de l'information en évolution rapide*

Que l'on soit journaliste ou citoyen, les médias sociaux permettent d'engager l'ensemble des parties prenantes à un évènement donné quelles que soient les mesures de blocage à la circulation de l'information.

- *préserver la diversité et la durabilité de l'écosystème européen des médias d'information*

Dans les environnements où la circulation de l'information pourrait être restreinte ou les sources contrôlées, toute population ayant accès aux médias sociaux est susceptible de faire entendre son témoignage, luttant ainsi contre le principe d'atomisation. L'atomisation ne fonctionne pas seulement en coupant les individus de ceux qui partagent les mêmes idées, mais en les empêchant même de croire qu'ils sont là-bas. Le modèle de communication « plusieurs-à-plusieurs » des médias sociaux est donc révolutionnaire d'un point de vue stratégique car il rend la possibilité de désatomisation réelle et évidente. (Sharp, 2011).

Les résultats du Darpa Twitter Bot Challenge propose la mise en place d'un processus semi-supervisé en trois étapes :

- détection initale de bot,
- clustering, mise en qualité, et analyse de réseau,
- classification et analyse des anomalies.

A chaque réseau, chaque évènement, les bots qui sont mis en œuvre ont un but spécifique. Il s'agit d'en identifier quelques-uns par les moyens suggérés. Le clustering permettra la détection d'autres bots ainsi que la qualification de comptes humains, la classification et l'analyse des anomalies ont pour but d'identifier leur contenu pour l'isoler du jeu de données.

Tout cette activité autour des Twitterbot ou des opérations d'influence est due à la façon dont les tweets sont affichés pour les utilisateurs : « *Le fait que Twitter affiche les tweets par ordre décroissant de publication limite les possibilités de promotion par tweet, car les tweets les plus récents sont ceux qui doivent être affichés dans les premières positions et le temps pendant lequel ils restent à ces positions dépend uniquement du nombre de tweets publiés dans les minutes suivantes.* » (Babaei et al., 2015). De ce fait pour garantir que ses idées soient vues par le plus grand nombre d'utilisateurs une organisation aurait intérêt à être présente voire à saturer le réseau sur une période longue au travers de système automatisés.

3.5. Conclusion

La première partie de ce chapitre a décrit comment les médias sociaux numériques ont conquis les utilisateurs quelles que soient leurs caractéristiques ethniques, sociales, éducatives. Lorsqu'il s'agit de se maintenir informé, là où ils sont disponibles, les réseaux sociaux surpassent les médias traditionnels en termes de volume, vélocité, variété et véracité caractéristiques du Big Data. Leur impact sur les sociétés connectées est tel qu'il est l'objet de très nombreuses études, cependant seul un nombre réduit de celles-ci les observent dans les situations de conflit. Parmi les recherches portant sur leurs rôles supposés ou avérés lors des mouvements sociaux qui ont secoués la dernière décennie, les conclusions divergent sur de nombreux points sauf un : ils sont un relai d'information sans comparaison au point de transformer le champ de bataille tel que le militaire en a l'habitude. Ce dernier opère désormais, et de plus en plus, sur un théâtre connecté où les parties prenantes mènent toutes une guerre info-centrée. Ce théâtre connecté n'est pas un espace d'affrontement qui surgit uniquement en période de guerre, il s'inscrit dans un conflit permanent fixé autour du concept de guerre hybride. Ainsi toutes les informations mises en ligne ne peuvent pas être prises en compte sans certains processus de traitement pour éviter les intoxications et opérations d'influence.

Conclusion de la première partie

Guerre hybride, continuum sécurité-défense, deux concepts décrivant une même réalité : la société civile, la base arrière de l'adversaire, est une cible permanente. Une des façons de l'atteindre est d'opérer sur son opinion publique, de créer des clivages, de faciliter la polarisation, voire de contribuer à la provocation d'un mouvement social. La fonction renseignement doit être en mesure de détecter les prémices de ce type de situation, de détecter les évènements. À cette fin, il nous paraît indispensable de développer les liens entre sciences humaines et sociales (SHS) et praticiens du renseignement. Dans cette partie, nous avons exposé comment les cadres théoriques des SHS trouvent une application concrète lorsqu'ils sont appliqués aux données de sources ouvertes en particulier celles issues des médias sociaux numériques. La méthodologie du « protest event analysis » (malgré ses travers) est une illustration de l'apport des SHS au renseignement de sources ouvertes, d'autant plus qu'elle est compatible avec les apports de l'intelligence artificielle. Le « protest event analysis » traditionnel est arrivé à ses limite et il doit évoluer à cause du contenu généré par les utilisateurs de l'internet. Les utilisateurs des réseaux sociaux numériques sont la fabrique de masse de l'évènement.

Partant du principe que les données de sources ouvertes permettent une meilleure compréhension du monde environnant, leur volume pose un problème d'exploitation qu'aucun humain ne sait résoudre. De ce fait, de nombreux projets en intelligence artificielle ont émergé pour permettre la prédiction de crise dans ce qui est qualifié de système de terrain humain. La modélisation du comportement individuel permettant l'identification d'insurgés parmi la population a été l'objet de nombreuses critiques et a généré une certaine déception tant parmi les militaires que parmi les politiques. L'approche par le comportement individuel relève d'une capacité de ciblage et non d'une capacité d'anticipation. Cette dernière n'est possible qu'au travers d'un suivi des faits pour en détecter ceux devenant des évènements. C'est à l'aune des évènements qu'il devient possible d'anticiper le cours de l'histoire. Reste à être en mesure de qualifier les faits en évènements, et d'assembler les évènements en base de données pour y appliquer une intelligence artificielle. Cette faculté ne peut s'envisager qu'au travers d'une refonte du cycle du renseignement par une intégration des capacités issues du Web pour le mettre en mesure de mieux utiliser les données de masse recueillies. Les services de renseignement ne peuvent plus se passer ni des outils de traitement des données de masse ni

des données issues des utilisateurs d'internet, mais pour en tirer des connaissances ils doivent repenser leurs méthodes d'exploitation.

La guerre hybride impacte l'ensemble des citoyens et il est nécessaire d'être en capacité d'intégrer les données générées par les utilisateurs du Web, notamment ceux des médias sociaux. Des techniques de préparation et d'exploitation analytique des données de masse permet d'en faire des jeux de données d'une plus grande fiabilité. Elles seront décrites dans la partie suivante. De plus, la volonté croissante du monde scientifique de partager des bases communes pour faire progresser les algorithmes d'analyse permettra une amélioration continue de la capacité d'anticipation.

Deuxième partie : Méthodologies de détection d'évènements. Le cas de la crise ukrainienne

Introduction de la deuxième partie

Notre postulat de départ, détecter les évènements plutôt que de chercher à prédire les insurrections, s'inscrit dans le travail sur les signaux faibles. Comme l'arythmie cardiaque peut être signe de maladie, les soubresauts d'une communauté sur un réseau social peut être une anomalie pouvant avoir valeur d'indicateur d'alerte. La détection d'évènement dans les médias est un sujet de recherche auquel est rompue la communauté scientifique depuis que les médias existent. Nous verrons comment les résultats de ces travaux se transposent aux médias sociaux dans le premier chapitre de cette deuxième partie. Nous regarderons en détail ce qu'est un tweet et comment la nature même de ce média permet une meilleure exploitation de l'information. Nous proposerons ensuite une méthode simple, DETEVEN, pour détecter un signal faible, un évènement, même lorsqu'il est noyé dans un flux aussi massif que le flot de tweet d'un pays en crise. Le second chapitre expliquera les dynamiques de cette crise. Nous inscrirons la chronologie des évènements dans le contexte de guerre hybride dont cette crise est l'exemple type repris par toutes les autorités, civiles comme militaires, sur le sujet. Pour clore ce chapitre, nous regarderons comment les parties prenantes ont utilisé Twitter pendant les différentes étapes de la crise : de la manifestation à la guerre civile. Le troisième chapitre quant à lui illustrera les apports de l'analytique. Cette pratique de l'analyse par le calcul est un prélude à l'application de l'intelligence artificielle sur le sujet de la détection d'évènement. Pour conclure cette deuxième partie nous montrerons que les analyses statistiques, sémantiques, et relationnelles, appuyées par des moteurs de règles eux-mêmes améliorés par des processus d'apprentissage, sont la méthodologie déployée pour traiter les données de masse en situation de recherche académique, de renseignement militaire, de sécurité intérieure.

4. Chapitre 4. Les algorithmes de détection

4.1. Introduction

La gestion de crise est la capacité à s'organiser en vue de limiter les impacts d'une situation exceptionnelle négative. Cette méthodologie d'action repose en partie sur la capacité à remonter l'information, déterminer les faits, estimer les impacts, mobiliser les équipes, gérer l'évènement et en retirer les leçons. À chacune de ces étapes, l'échange d'information est une condition indispensable au succès. In fine, la gestion de crise repose sur une chaîne de transfert d'information entre toutes les parties prenantes dont la première étape est la détection de l'évènement et la dernière le retour à une situation normale. La première étape de la gestion de crise est la détection de la crise elle-même, la seconde, la plus complexe, est le suivi de situation. Ces deux étapes nécessitent une capacité à détecter les évènements constitutifs de la crise. En effet, cette dernière s'inscrit immédiatement dans un environnement informationnel saturé qui complique la détection des évènements permettant d'avoir une image fidèle de la situation sur le terrain. Le suivi de situation de crise s'appuie sur une analyse chronologique des évènements dans un environnement donné. L'objectif est de regrouper l'intégralité des informations portant sur un évènement (approche quantitative) et d'en exploiter le contenu au travers de séries temporelles (approche qualitative). La crise et ses évènements constituants impactent les personnes qui de plus en plus s'expriment sur les médias sociaux. Ce média étant difficilement censurable, il présente un intérêt particulier pour la détection d'évènements.

Notre étude porte sur l'utilisation de Twitter pendant le conflit ukrainien, c'est-à-dire un moment où le réseau est saturé de termes portant sur la révolution, les affrontements armés, le conflit sous toutes ses formes. Dans cet environnement informationnel chargé, nous cherchons une méthodologie permettant de détecter les évènements, quels qu'ils soient, et de voir si ces derniers permettent effectivement le suivi des soubresauts du conflit. Notre approche se base sur la déclaration de géolocalisation ou mention de toponyme par l'émetteur. Il est question de savoir comment détecter les moments de tensions et de déterminer si la proximité géographique de l'émetteur influe sur la précision ou le délai de détection.

4.2. Qu’est-ce qu’un tweet ?

Un tweet peut contenir, dans la limite de 240 caractères (140 entre 2006 et 2017) de l’information textuelle, des liens vers d’autres médias, la mention d’un twittos. Il peut être émis, retweeté, mentionné. Plus que les caractères qui apparaissent dans le corps du texte, un tweet contient de multiples informations. En effet le corps du texte (en orange ci-dessous) n’est qu’une infime partie des données diffusées.

Lorsque le tweet suivant apparait sur le flux chronologique de Twitter : « SHS & SIC pour le continuum sécurité-défense ! @oak http://oakbranch.fr/success_stories »#SIC #SHS #SECURITE #DEFENSE ; en réalité, l’information disponible est beaucoup plus riche, voir figure 5.

Avant d'explorer les données, il est important de connaître la structure d'un tweet restitué par l'API Twitter ou par le fournisseur des données lorsqu’elles sont achetées (auprès de Twitter ou autre fournisseur de données, voir figure 6.

Comme nous l’expliquerons ci-après l’ensemble des éléments composant un tweet, son contenu, ses métadonnées, et le contexte de diffusion (relation de l’émetteur avec son audience) peuvent contribuer à la détection d’un évènement. À titre d’illustration complémentaire, si l’on considère uniquement la métadonnée « actor » qui caractérise l’émetteur du tweet. Cette métadonnée est complétée par les éléments suivants :

- person : distinction entre entité physique ou morale
- id : identifiant unique
- link : vers un site appartenant à l’actor
- displayName : nom affiché
- postedTime : heure de diffusion
- image : image représentant l’Actor
- summary : texte de remplacement du tweet, par défaut copie du texte
- links : lien vers le profil déclaré de l’Actor
- friendsCount : nombre de comptes auquel l’Actor est lié
- followersCount : nombre de comptes abonnés à l’Actor
- listedCount : nombre de fois que le compte de l’Actor apparait dans une liste
- statusesCount : nombre de tweet émis par l’Actor

- twitterTimeZone : fuseau horaire de l'Actor
- verified : si l'actor a fourni à Twitter des éléments supplémentaires d'identification
- utcOffset : format d'heure
- preferredUsername : nom d'utilisateur préféré, peut être différent du displayName
- languages : langues utilisées par l'Actor
- location : position déclarée dans le profil de l'Actor

L'actor est le centre d'intérêt du chercheur dès que l'on s'intéresse aux individus et pas seulement à leur émission, notamment dans l'identification de communauté ou de botnets. Pour caractériser un évènement, il peut être nécessaire de savoir quels sont les actors les plus actifs, les plus suivis, ceux qui suivent le plus, est-ce qu'un même « displayname » ou une même image, un même « actor_href », « actor_rel » ou le même « actor summary » existe chez d'autres actors (indication de communauté ou de botnet). Le suivi de l'évolution des « listedCount » ou « statusesCount » permet de mesurer l'activité d'un actor, d'identifier ainsi des ruptures d'habitudes, des croissances exponentielles, etc. Les dates de créations d'actors sont des bons indicateurs, elles permettent d'identifier si des actors ont été créés au même moment et en recoupant avec les « timeZone », les « utcOffset » et la « location », de voir s'ils ont été créés au même endroit. La « location » permet de voir si les toponymes retrouvés dans l'ensemble des tweets d'un actor correspondent à la location déclarée, si l'actor twitte au sujet d'une zone géographique de prédilection. L'utilisation d'un gazetteer et de la détection de topic permet de prédire la probabilité quels actors sont susceptibles de fournir les premiers éléments d'information quand un évènement à lieu dans une zone déterminée La prise en compte de la langue affichée peut être comparée à la langue dans laquelle sont émis les tweets.

```
{
  "verb": "post",
  "postedTime": "2016-10-21T16:02:46+00:00",
  "body": " SHS & SIC pour le continuum sécurité-défense ! @oak http://oakbranch.fr/success_stories",
  "twitter_entities": {
    "urls": [
      {
        "expanded_url": null,
        "url": "http://oakbranch.fr/success_stories",
        "indices": [
          69,
          100
        ]
      }
    ],
    "hashtags": [ [{"text":"SIC","":"SHS","":"SECURITE","":"DEFENSE"
    ],
    "user_mentions": [@fanch
      {
        "name": "OAK, Inc.",
        "id_str": "16958875",
        "id": 16958875,
        "indices": [
          25,
          30
        ],
        "screen_name": "OAK"
      }
    ]
  },
  "actor": {
    "location": {
      "displayName": "Paris, FR",
      "objectType": "place"
    },
    "postedTime": "2016-10-24T23:22:09+00:00",
    "displayName": "OAK, Inc.",
    "preferredUsername": "oak",
    "utcOffset": -25200,
    "objectType": "person",
    "statusesCount": 302,
    "languages": [
      "en"
    ],
    "listedCount": 23,
    "links": [
      {
        "href": "http://blog.oak.fr",
        "rel": "me"
      }
    ],
    "friendsCount": 71,
    "followersCount": 260,
    "summary": "Open actionable intelligence.",
    "link": "http://oakbranch.fr/boom",
    "image": "http://a3.oak.com/profile_images/62993643/icon_normal.png"
  },
  "objectType": "activity",
  "id": "tag:search.twitter.com,2008:28039652140",
  "link": "http://twitter.com/oakbranch/statuses/29039652140",
  "generator": {
    "displayName": "web",
    "link": "http://twitter.com"
  },
  "object": {
    "postedTime": "2013-10-21T16:02:46+00:00",
    "id": "tag:search.twitter.com,2005:28039652140",
    "objectType": "note",
    "link": "http://twitter.com/oakbranch/statuses/28039652140",
    "summary": " SHS & SIC pour le continuum sécurité-défense ! @oak
http://oakbranch.fr/success_stories "
  },
  "provider": {
    "displayName": "Twitter",
    "objectType": "service",
    "link": "http://www.twitter.com"
  }
```


Figure 6 : Code json d'un tweet

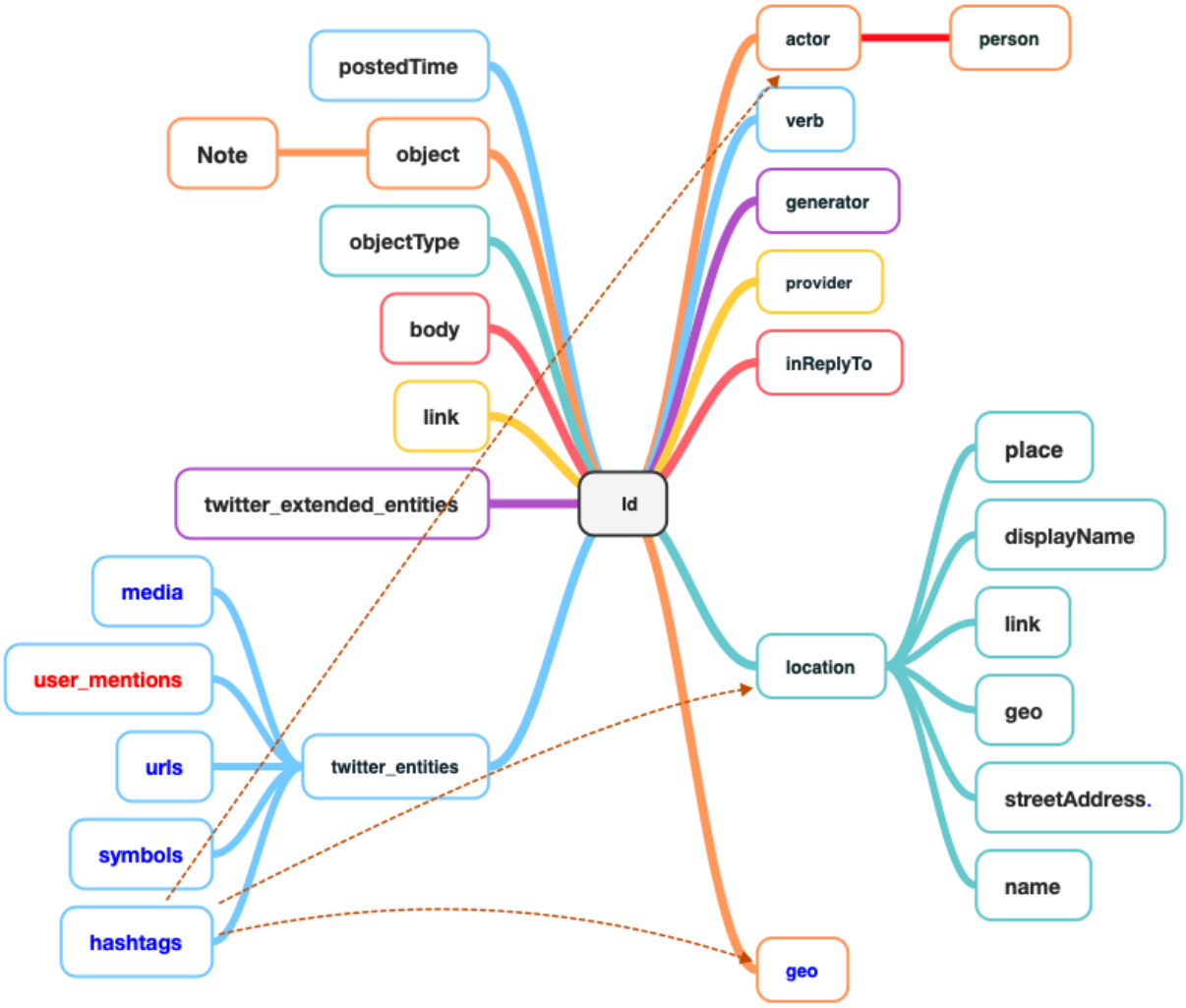


Figure 6b : Cartographie des composants d'un tweet, voir le détail en annexe 2

Il existe de très nombreuses études portant sur la collecte de tweets au travers des Application Programming Interface (API) de Twitter. Une API est un programme permettant aux utilisateurs d'interagir avec un type de technologie. L'intérêt est de promouvoir l'innovation externe, renforçant encore la technologie de base, le service ou les données. Offrir des données en externe permet aux développeurs de créer des produits, des plates-formes et des interfaces sans avoir à exposer les données brutes qui restent contrôlées en interne. Il est courant que les entreprises technologiques laissent se développer puis acquièrent d'autres technologies innovantes plutôt que de créer des innovations en interne. Twitter a capitalisé sur ce modèle, comme en témoigne l'acquisition de dizaines sociétés de technologie différentes, construites autour de leur API ouverte.

L'API SEARCH/REST de Twitter : permet de collecter des Tweets basés sur des paramètres spécifiques tels que des mots-clefs ou des noms d'utilisateurs ou des lieux. Cela ne vous donne pas de données en direct, mais permet de collecter pour de l'analyse sur les données historiques.

Avec l'API SEARCH, il est possible d'obtenir les tweets qui ont été émis avec un nombre maximal de tweets correspondant aux 3 200 derniers tweets, quels que soient les critères de la requête. Avec un mot clé spécifique, on ne peut généralement interroger que les 5 000 derniers tweets par mot clé. Il existe également une limitation par le nombre de demandes qu'il est possible d'effectuer au cours d'une période donnée. Les limites des demandes Twitter ont changé au fil des ans, mais sont actuellement limitées à 180 demandes par période de 15 minutes.

L'API STREAM de Twitter : diffuse en continu des tweets correspondants aux critères de recherche jusqu'à ce que vous lui demandiez d'arrêter. Ceci est particulièrement utile lorsque le but est d'analyser des campagnes en direct sur Twitter. L'inconvénient majeur de l'API STREAM est qu'elle ne fournit qu'un échantillon des tweets en cours. Le pourcentage réel du nombre total de tweets reçus par les utilisateurs avec l'API de diffusion en continu de Twitter varie considérablement en fonction des critères définis par les utilisateurs et du trafic actuel. Des études ont montré que l'utilisation de l'API de streaming de Twitter permettait aux utilisateurs de recevoir entre 1% des tweets et plus de 40% des tweets en temps quasi réel, mais sans maîtriser les critères de sélection des tweets transmis.

Ces API, gratuites, sont en constante évolution et il est d'autant plus difficile de garantir des résultats de collecte qu'elles sont limitées pour ne pas concurrencer l'offre commerciale de Twitter. A titre d'indication, les API Premium (à mi-chemin entre l'offre gratuite et l'offre Enterprise) coûtaient en 2017 entre 149 et 2,499 dollars par mois, en fonction du niveau d'accès requis (Twitter, 2019). Comme l'explique une entreprise spécialisée dans la vente de données Twitter : « *Lorsque vous extrayez tous les tweets d'un utilisateur unique* […]*, la requête doit être exécutée sur les 500 millions de tweets de la journée pour trouver ceux qui proviennent de cet utilisateur spécifique. La recherche d'informations dans cet environnement est un processus de calcul intensif. Tous les systèmes fonctionnent dans un cloud commercial. Il existe des programmeurs dans plusieurs organisations, des gestionnaires de bases de données, des avocats, des comptables, de nombreux fournisseurs d'hébergement en nuage, des coûts de calcul, d'électricité et de bande passante, pour ne nommer que quelques-uns des facteurs qui ont une incidence sur le prix. Vous pouvez donc obtenir pendant un an des tweets utilisateur, mais il faut interroger 365 x 0,5 milliard de lignes de données. Si vous comparez des caractéristiques de métadonnées ainsi que le corps du Tweet, nous parlons de milliers de milliards de cellules pour interroger et extraire des informations.* » (Sifter, 2018)

Avant de pouvoir exploiter les données issues de Twitter, il est nécessaire de définir un modèle de données et de les mettre en base. Le résultat de l'intégration de ces données complexifie nettement le traitement et la mise en qualité des méga-données. Il est donc question de mettre en œuvre des processus d'échantillonnage, de préparation, modélisation, de mise en qualité des données, préalablement à toute intégration et exploration dans des systèmes automatiques ou assistés. Le modèle de donnée doit être défini avec beaucoup d'attention et en parallèle, le rendre flexible aux changements qu'il connaitra au fur et à mesure de l'évolution des questions de recherche. L'objectif de l'étude du jeu de données est de comprendre :

- Pourquoi les gens utilisaient Twitter ?
- De quoi parlaient les gens sur Twitter ?

Sur une période de huit mois, le travail portera sur l'évolution de ces deux questions en fonction des changements de situations dans l'environnement. Le jeu de données sera analysé sémantiquement pour catégoriser les tweets par ensemble homogène. Une fois les grandes catégories définies, nous avons effectué une étude de l'évolution de la volumétrie sur la durée et une étude des métadonnées pour analyser les rapports suivants :

- Rapport entre la proximité géographique avec l'évènement et les termes employés
- Rapport entre la proximité temporelle avec l'évènement du tweet et les termes employés
- Mode de diffusion de l'information : analyse des réseaux sociaux
- Vitesse de propagation d'une information
- Mesure de popularité d'un tweet
- Impact émotionnel de l'évènement

Un modèle de données est un ensemble de tables reliées entre elles contenant des variables sur lesquelles sont appliquées des procédures. En principe toutes les données pourraient tenir dans une seule table. Cependant pour augmenter la flexibilité et la vitesse d'exécution des traitements il est utile de créer autant de tables que pertinent en prenant en comptes les questions de recherche (bien que cela est un impact significatif sur l'infrastructure machine). Le résultat de l'intégration de ces données complexifie nettement le traitement et la mise en qualité des méga-données. Il est donc question de mettre en œuvre des processus d'échantillonnage, de préparation, modélisation, de mise en qualité des données, préalablement à toute intégration et exploration dans des systèmes automatiques ou assistés. Pour exemple, les 10 millions de tweets de notre jeu de données pesaient un peu plus de 4 gigas à réception, mais une fois déployé dans les bases de données d'exploitation le volume est monté à plus de 175 gigas.

L’ensemble de ces indicateurs sont à avoir à l’esprit quand on se lance dans la détection d’évènements sur Twitter.

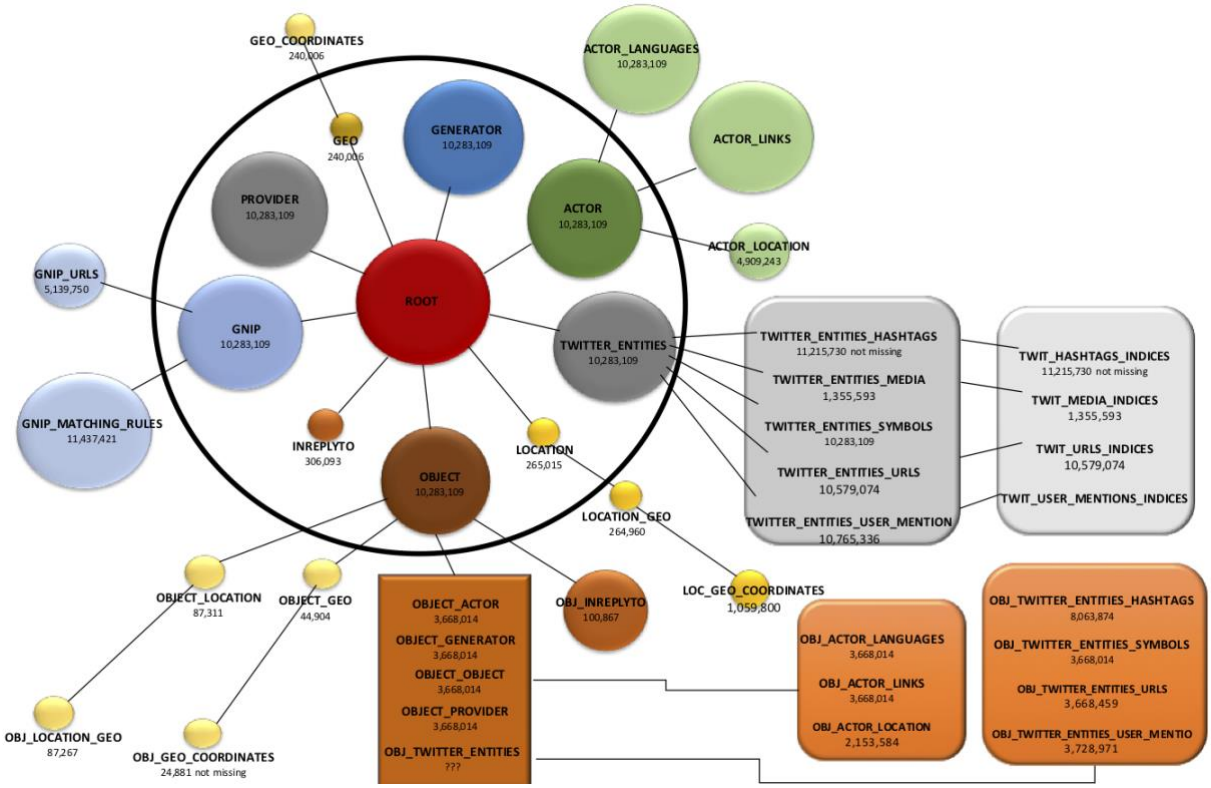


Figure 7 : Modèle de données DETEVEN

4.3. État de l'art des algorithmes de détection

La détection d'évènement s'applique à de nombreux domaines et sur de nombreux jeux de données. Il peut s'agir de détecter des épidémies dans des données médicales, des vagues de crimes dans des données policières, ou plus simplement des anomalies par rapport à une norme. La détection requiert deux conditions : qu'une norme soit définie, que des critères de déviance par rapport à la norme soient observables. Nous nous intéresserons spécifiquement à la détection d'évènements dans les médias sociaux et plus particulièrement sur twitter en situation de conflit.

La détection d'évènement dans les données issues de Twitter est particulièrement complexe dû aux spécificités du flux qui est fragmenté et bruyant, d'une grande variété et répétitif (Zhou et al., 2015). Encore faut-il s'entendre sur la notion d'évènement. Pour le suivi d'une situation de conflit, nous considérons un évènement comme une séquence de faits chrono-géo-référencé, se distinguant des faits en cours ou prévus et ayant un impact remarquable sur les faits à venir. Comme annoncé dans l'introduction générale, ce qui distingue un évènement d'un non-évènement est le rapport aux hommes. Un évènement touche donc les hommes et ses derniers en parlent. Un évènement c'est donc du discours, des mots qui permettent de le détecter, ou dans un premier temps de repérer le fait dont l'impact pourra en faire un évènement. Un évènement est une crise, une rupture de l'équilibre, un décalage par rapport à la norme : *« l'idée de perturbation est la première que fasse surgir le concept de crise […] ce peut être l'évènement, l'accident, la perturbation extérieure qui déclenche la crise.* » (Morin, 1976).

Une grande majorité d'études sur l'utilisation de Twitter en période de crise s'intéresse aux catastrophes naturelles. Peu ont pour sujet des conflits sociaux violents et encore moins de conflits armés, malgré des travaux remarqués sur les conflits du printemps arabe (Lotan et al., 2011 ; Bruns et al. 2013). Dans leur revue des pratiques des mégadonnées et de la gestion de crise, Raza et ses collègues ne citent que des catastrophes naturelles en référence (Raza et al. 2019). Sur les études portant sur les catastrophes naturelles, dans la phase détection et suivi de situation, les médias sociaux sont la deuxième source d'information pour le suivi de situation (Yu, et al., 2018).

Comme pour les catastrophes naturelles, un affrontement armé s'inscrit dans la durée, mais la nature de l'information contenue varie grandement pour deux raisons : d'une part, il alterne des phases de tensions et de détentes, d'autre part les parties prenantes se livrent à une intense

guerre d'information. La fiabilité des médias sociaux lors de catastrophes naturelles est régulièrement remise en question : « *L'inégalité sociale et spatio-temporelle dans l'utilisation des données des médias sociaux devrait être pleinement prise en compte avant que ces données puissent être utilisées pour prévoir les dommages, enquêter sur les populations touchées et hiérarchiser les activités au cours de la gestion des catastrophes.* » (Huang et Xiao, 2015).

Dans le contexte d'un conflit armé, l'objet de notre analyse porte sur la détection d'évènements significatifs qu'importe la nature de l'émetteur ou son opinion. Malgré les différences affichées dans la nature de données entre une catastrophe naturelle et un conflit armé, l'objectif de suivi de situation reste le même, créer une capacité « *de connaissance collective, par exemple pour cartographier les zones affectées, évaluer les dégâts et diffuser rapidement des informations, et en mode passif, comme collecter les tweets dans un théâtre humanitaire, pour améliorer un système d'alerte précoce et mieux comprendre l'offre et la demande [de soins].* » (Kibanov, et al., 2017).

Lorsque la crise à un fort impact humain (catastrophe naturelle, industrielle, guerre) la grande connectivité que permettent les NTIC implique la création et le relais d'une masse d'informations émise tant par les sinistrés, les autorités, les sympathisants, etc. Ce volume massif entraîne comme « risque principal est d'être noyé par un tel tsunami numérique, de ne pas réussir à isoler les informations importantes dans un flot de messages insignifiants » auquel il faut ajouter deux autres vulnérabilités pendant la crise : capacité de nuire (fake news) ; atteinte à la vie privée (Hecker, 2014). Les premières étapes de diffusion de l'information en temps crise étant l'alerte et le suivi de situation (également appelée image opérationnelle commune, IOC), il parait opportun de déterminer quels dispositifs permettraient de détecter une crise et de contribuer à la tenue de la situation tactique des sous-évènements grâce aux médias sociaux et ce avec le plus grand degré d'automatisme. Il existe de multiples formes de remontée d'information. Cependant dès lors qu'une crise à un impact sur l'opinion publique, les médias sociaux sont depuis 2006 le médium privilégie de diffusion de l'alerte. Qu'il s'agisse d'un dispositif institutionnel tel que la diffusion d'alerte de tremblement de terre et/ou de tsunami ou de réaction citoyenne à des incidents violents, Twitter est massivement utilisé dans les situations de crise pour alerter la population d'évènements à haut niveau d'impact.

Dans une situation de crise, pour qualifier l'utilité d'une information, il faut être en mesure d'estimer trois critères du couple émetteur/information : la proximité temporelle (primo diffuseur ou relais), la proximité géographique du témoignage (direct ou indirect), la proximité thématique (dans le sujet ou hors sujet). Il est question de savoir si l'émetteur parle bien de la

crise, l'émetteur est un témoin direct, l'information est une alerte avancée. Ces critères peuvent être ensuite déclinés. Par exemple l'information ne parle pas directement de la crise, mais de la zone en général, l'émetteur n'est pas un témoin direct, mais sa source l'est, l'information n'est pas une alerte avancée, mais permet un recoupement.

Trois grandes rétrospectives des pratiques de détection d'évènements sur Twitter ont été réalisées entre 2013 et 2018.

Farzindar Atefeh et Wael Khreich en 2013 (publié en 2015) ont recensé 16 études réalisées entre 2009 et 2012 sur ce sujet. Ils les ont classés entre celles qui cherchaient à détecter des évènements a posteriori (retrospective event detection) et celles qui cherchaient à détecter les évènements au plus près du temps réel (new event detection). Les évènements sont soit spécifiés, soit non spécifiés. La notion d'évènement est très vague : « *les évènements peuvent être définis comme des occurrences du monde réel qui se déroulent dans l'espace et le temps* », car elle s'inscrit dans la continuité des programmes de recherche sur la détection d'évènement et le suivi des sujets dans les médias (Topic Detection and Tracking, TDT) de l'agence de recherche de défense américaine la DARPA antérieure aux réseaux sociaux. Ce programme de recherche classe les informations de la façon suivante : un ensemble d'information devient un évènement, un ensemble d'évènements deviennent un sujet. Ce programme était destiné à identifier des sujets d'intérêts dans les flux d'information continue. La détection est de deux types : la détection rétrospective d'évènements qui agrège les tweets autour d'évènements connus pour pouvoir en suivre l'évolution et la détection d'évènements nouveaux qui doit décider si l'évènement détecté doit être agrégé à un cluster préalablement identifié ou s'il faut créer un nouveau cluster. Deux techniques sont utilisées pour détecter ces évènements dans le flux de Twitter : les méthodes qui représentent les documents en tant qu'éléments à regrouper à l'aide d'une mesure de similarité appelée document-pivot en anglais et les méthodes reposant sur la détection de schémas anormaux dans l'apparence des mots appelées feature-pivot. Atefeh et Kreich classent les méthodes en supervisées et non-supervisées. Dans les méthodes non-supervisées ils appellent à un regroupement des tweets en cluster plus fragmentés et une meilleure prise en compte de métadonnées pour améliorer ce regroupement. Ils ne recommandent pas les méthodes supervisées les considérants trop statiques par rapport à la fréquence d'émission et la variété des sujets commentés sur Twitter. De plus, ils reprochent à ces méthodes d'être entrainées sur des jeux trop restreints. Enfin parmi les axes d'amélioration à venir, ils considèrent que les performances doivent être mesurables en termes de précision et

de rappel, et les méthodes non limitées à la détection de mot en langue anglaise. (Atefeh et Kreich, 2013).

Mario Cordeiro et Joao Gama, en 2016, ont recensé 34 études réalisées entre 2008 et 2012 dont l'objet est la détection d'évènement sur Twitter. Ils reprennent la même définition de l'évènement que dans le programme de la DARPA où : « une histoire est "un segment d'actualité cohérent qui comprend deux ou plusieurs clauses indépendantes déclaratives au sujet d'un même évènement" ; un évènement est "quelque chose qui se produit à un moment et en un lieu précis, avec toutes les conditions préalables nécessaires et les conséquences inévitables" ; un sujet est " un évènement ou une activité phare, ainsi que tous les évènements et activités qui y sont directement liés. ». De nouveau on observe une certaine confusion possible sur ce qu'est un évènement. Dans ce cas il peut être à la fois significatif et insignifiant. Dans cette étude, le sujet est le concept qui s'approche le plus de notre définition de l'évènement. Comme pour la rétrospective d'Atefeh et Kreich, il est question de s'inscrire dans le contexte du Topic Detection et Tracking de la DARPA et de l'appliquer au flux Twitter. Leur détection d'évènement est faite soit par proximité sémantique du message (pivot de document) soit par la fréquence d'apparition ou l'anomalie de présence (pivot de caractéristiques). Parmi les méthodes les plus employées, il est fait mention du clustering basé sur la sémantique des corps de texte d'un tweet (body), des hashtags, pour la détection de nouveautés comme pour la détection rétrospective. La classification est employée principalement pour la détection rétrospective supervisée autour de sujets connus, renforcée avec des filtres forts. La détection des pics d'apparence de mots est également largement employée pour détecter les tendances et les évolutions d'un évènement. Pour les auteurs, les méthodes employées issues de concept mis au point pour les médias traditionnels et adaptés pour Twitter ne sont pas encore optimisées pour les enjeux de vitesse et de diversité de ce flux. (Cordeiro et Gama, 2016).

Manos Schinas, Symeon Papadopoulos, Yiannis Kompatsiaris et Pericles Mitkas, en 2018, ont analysé 36 études portant sur la détection d'évènement entre 2005 et 2017. Comme pour les deux autres rétrospectives, la détection porte sur des évènements passés et des évènements nouveaux. Aux méthodes document-pivot et feature-pivot, ils ajoutent une troisième méthode appelée modélisation de sujet (topic modeling) qui consiste à considérer les évènements : « *comme variables latentes dans les documents*. ». Non seulement les mots dans le texte sont des variables observables, mais aussi d'autres entités telles que l'utilisateur qui a posté le document, les mots extraits d'images publiées, les références spatio-temporelles du tweet le sont également. Selon les auteurs, les détections utilisant la méthode feature-pivot sont limitées par

le besoin de connaître le comportement passé d'un mot pour détecter l'anomalie que représente sa présence dans le flux. De ce fait elle n'est pas adaptée au temps réel et requiert un large volume de documents. Si cette méthode à propension à détecter les tendances, elle n'est pas en mesure de détecter les évènements non populaires. Quant à la méthode document-pivot, ell est plus adaptée aux médias classiques et à leur charge sémantique. Or les médias sociaux utilisent plus que des mots, ils utilisent des images, des liens, et disposent d'autres informations, les métadonnées de relations entre utilisateurs par exemple qui ne sont pas exploitées dans la détection. Enfin la méthode du topic-modeling est utilisée soit comme une étape préalable à la méthode document-pivot pour en améliorer la précision, soit dans le traitement de l'ensemble des données et des métadonnées pour contribuer à la détection d'évènement. (Shinas et al., 2018).

Nous ajoutons les remarques suivantes aux constats exprimés par les auteurs.

Tout d'abord, la notion d'évènement est très vague. Le centre d'intérêt de ces études, n'est pas tant de détecter les évènements, mais de distinguer les occurrences du monde réel (que nous considérons comme des faits et non un évènement) du bavardage et des rumeurs ayant lieu sur Twitter. L'évènement est représenté par une agglomération de tweets autour d'un sujet. La majeure partie des études établissent une sélection forte des données en entrée soit par requête sur l'API de Twitter, soit par sélection (et donc exclusion) des composants d'un échange de tweet étudiés (par exemple hashtag et/body du tweet, élimination des retweets, etc.).

La détection d'évènement sur Twitter par les études compilées dans les trois rétrospectives s'inscrit dans la continuité (et font référence au) Topic Detection and Tracking (TDT) (Allan, 2002). Ce programme a été financé entre 1996 et 1998 par la Defense Advanced Research Projects Agency (DARPA), l'agence pour les projets de recherche avancée de défense américaine chargée de la recherche et développement des nouvelles technologies destinées à un usage militaire. Si cela montre l'intérêt indéniable des militaires pour le sujet de la détection d'évènement, le contexte de ce programme limite son intérêt pour Twitter. Tout d'abord le programme avait vocation a détecter les évènements dans un flux multi-sources, limité aux information/actualités (news) seulement. Même si l'on peut considérer Twitter comme un réseau où chaque utilisateur est une source, on ne peut estimer que son contenu soit aussi homogène qu'une chaîne d'information.

Nous constatons que la très grande majorité des études se sont basées sur l'API STREAM de Twitter, c'est-à-dire que les données sont recueillies sans maîtrise de l'algorithme

d'échantillonnage que Twitter maintient secret. De plus, les études portant sur une période allant de 2009 à 2017, les fonctionnalités de l'API et l'algorithme d'échantillonnage ont été significativement modifiés à de nombreuses reprises rendant les résultats difficilement comparables et réplicables.

Les études se limitent à traiter le contenu du tweet et non l'ensemble des données disponibles. L'utilisation des métadonnées reste minimale, elles sont employées pour améliorer le processus de clusterisation, mais ne sont en général pas employées comme déclencheur de détection. Or comme nous l'avons illustré dans la première partie de cet article un tweet est beaucoup plus que la somme d'un texte et d'un hashtag.

On observe une étanchéité entre la détection a posteriori et la détection en temps réel. Les méthodes employées pour la détection rétrospective ne sont pas conçues pour être transférables vers le temps réel par leurs auteurs.

Enfin, la détection n'est pas une catégorisation : le rassemblement de groupes de faits différents par critères de similitudes en cluster ne permet de distinguer les évènements des clusters de faits. L'apprentissage machine basé strictement sur les critères des clusters ne permet de détecter les évènements, car les faits normaux sont beaucoup plus fréquents que les faits anormaux. Les évènements ne sont pas des faits aux critères aberrants, il s'agit de faits dont l'impact change les faits qui suivent.

4.4. La méthode DETEVEN

En situation de crise, l'information idéale serait, sur Twitter, un tweet :

- diffusant une information sur l'évènement
- au moment de la survenue de celui-ci
- geotaggé, c'est-à-dire dont la géolocalisation est inscrite dans les métadonnées du tweet par le moyen de géolocalisation du téléphone au moment de l'émission

Les tweets réunissant ces trois caractéristiques sont non seulement rares, mais également plus difficiles à détecter dans le flux de données.

Si la proximité temporelle est essentielle dans la phase d'alerte d'une crise, elle devient secondaire dans la phase de gestion. En effet, il est plus pertinent d'utiliser comme critères de collecte la proximité thématique et géographique pour identifier les tweets d'intérêt comme venant d'une zone de crise et parlant d'une crise. La proximité temporelle est plus souvent une qualité attribuée a posteriori et permet surtout d'ordonner les tweets collectés lors de la phase de gestion.

Les deux défis de la collecte deviennent alors l'attribution de la proximité thématique et de la proximité géographique des tweets.

La proximité géographique d'un émetteur diffusant de l'information sur une crise en cours est possible directement si :

- L'émetteur a activé la géolocalisation de ses tweets
- L'émetteur s'est signalé à un endroit géolocalisé par des applications tierces compatibles avec Twitter telles que Foursquare ou Yelp à proximité de l'évènement
- L'émetteur a déclaré une position dans son profil ou dans un des tweets

La géolocalisation des émetteurs est le sujet de très nombreuses études. Deux études ont estimé le pourcentage de tweets géotaggés à 1% (Cheng et al. 2010 ; Morstatter et al., 2013 ; Sloan et al. 2013), c'est-à-dire des tweets dont la position d'émission est inscrite en métadonnées à partir de la géolocalisation GPS du dispositif d'émission, en général un téléphone portable. Il s'agit donc d'une minorité d'émetteurs dans le flux, la plupart des utilisateurs n'activant pas cette fonction pour des raisons de respect de vie privée. Cette métadonnée est donc très rare et devient un filtre très voire trop restrictif pour collecter un jeu de donnée qi la contienne, pertinent pour la détection d'évènement. Cependant : « *Les chercheurs utilisant ces informations peuvent être assurés qu'ils travaillent avec un échantillon presque complet de données Twitter lorsque des*

zones de limites géographiques sont utilisées pour la collecte de données. » (Morstatter et al., op. cit.). Il n'existe pas de données sur le pourcentage d'émetteur géolocalisé par applications tierces, mais pour les mêmes raisons de protection de la vie privée, leur volume restera très faible. Cette fonction de pouvoir attribuer une géolocalisation d'un tweet est tellement peu utilisée qu'en juin 2019 Twitter la retire tout simplement : « *La plupart des gens ne marquent pas leur emplacement précis dans Tweets, nous supprimons donc cette possibilité de simplifier votre expérience de Twitter. Vous serez toujours en mesure de marquer votre position précise dans Tweets grâce à notre appareil photo mis à jour. C'est utile lorsque vous partagez des moments sur le terrain.* ». (@TwitterSupport, 2019). Malgré tout, le déplacement de la fonction dans l'outil d'appareil photo intégrée dans l'application pour « partager des moments sur le terrain » reste intéressant. Le rapport qu'ils estiment utile entre le moment et le terrain est proche de notre rapport entre de l'évènement et le lieu.

Reste donc la dernière option, la géolocalisation par analyse sémantique des données. Le positionnement en fonction des données de profils est sujet à caution, car les données peuvent ne pas être actualisées. La proximité géographique par déclaration de géolocalisation semble le moyen le plus utile pour géolocaliser un émetteur en période de crise susceptible d'être une source pertinente pour détecter un évènement.

Parmi les mots employés pour parler de l'évènement, il y a une catégorie qui nous a paru révélatrice d'évènements : les toponymes. Le toponyme est à la fois le nom d'un lieu, mais également son repère géographique. Les lieux c'est à partir de quoi s'ancre les évènements. Le lieu dans le discours c'est l'endroit dont parlent et d'où parlent les parties prenantes à l'évènement. En crise, l'évènement est lié à un lieu dont parlent les gens, le lieu cristallise la volonté de témoigner des parties prenantes à l'évènement.

Partant de ce postulat, l'objectif est de détecter un évènement par la mention de toponymes. L'intérêt de ce type de mot est qu'il s'agit d'une liste finie. Même en prenant en compte l'ensemble des translittérations ukrainienne, russe et anglaise, la liste des villes d'Ukraine est invariable. De plus, la détection par un classificateur binaire est extrêmement rapide et se prête à la haute volumétrie et à la célérité d'un flux comme celui de Twitter (une moyenne de 180 000 tweets par jour pendant la période observée).

D'autres méthodes que la détection de toponymes sont possibles pour géolocaliser une émission. Il est possible d'inférer la position d'un émetteur en déduisant sa géolocalisation de métadonnées d'autres tweets (reply to @ d'une personne elle-même géolocalisée). Si une recherche « *de géolocalisation peut être considérée comme une tâche de régression par rapport*

aux coordonnées géographiques réelles, ou une tâche de classification sur des emplacements régionaux discrétisés » (Rahimi et al., 2015) qui se traduit par une classification basée sur le texte pour détecter des mentions de lieu ou une régression basée sur la localisation des membres du réseau étant entendu que les personnes interagissent plus avec les membres géographiquement proches. Toutefois cette dernière méthode nécessite cependant un large volume de donnée, voire une collecte extensive des échanges d'un utilisateur et de son réseau pour estimer sa position. Une autre étude a démontré sa capacité à détecter la présence d'un émetteur dans une zone de crise en analysant la façon de s'exprimer sur la crise à partir d'une séquence linguistique (détection de prépositions de lieu et Part of Speech tag). Il en résulte que sur l'ensemble des tweets émis sur la crise, il est possible de distinguer ceux qui viennent de l'intérieur de la zone impacté de ceux qui en sont à l'extérieur (Mortsatter et al, 2014).

La détection de toponymes dans le corps de texte dépasse la géolocalisation des émetteurs, elle permet d'identifier les tweets dont les auteurs ont utilisé une partie du nombre très limité de caractères autorisés (140 caractères au moment des faits) pour s'assurer que ce qu'ils relatent soit bien identifié comme se rapportant à un lieu précis.

Dans le contexte de nos travaux, il fallait obtenir le maximum de tweets sur le conflit ukrainien. Seule l'API SEARCH était disponible gratuitement et au vu des limitations incompatibles avec l'objectif de nos travaux (en particulier la non-maîtrise du processus d'échantillonnage), nous avons décidé d'acquérir les données auprès de Twitter. Avec un objectif de travail au plus près des témoins directs des évènements donc il fallait obtenir uniquement les tweets en russe ou ukrainien. Pour des raisons financières, il n'était pas possible d'obtenir les 28 millions de tweets émis en russe et en ukrainien sur la période du 1/11/13 au 1/11/14. Nous avons décidé d'un premier filtre mis en place pour limiter la collecte aux tweets mentionnant un toponyme d'une ville en Ukraine ou d'une rue de Kiev (voir liste en annexe 3). Le résultat fut une première découverte sur le jeu de donnée : malgré ce filtre très restrictif il restait 22 millions de tweets, soit près de 78% de tous les tweets émis sur la période. Afin de limiter plus encore le volume et le coût associé, la période a été réduite du 1/11/13 au 1/06/14, une période de 212 jours pour un résultat de 10 millions de tweets dont le profil d'utilisateur ou le contenu ou une métadonnée de géolocalisation contiennent le nom d'une ville ukrainienne ou d'une rue de Kiev.

Pour détecter les évènements par le suivi de mention de toponymes dans le flux, la principale difficulté vient de la non-propreté des documents du corpus Twitter. Il y a de nombreuses erreurs syntaxiques, fautes d'orthographe et de bruit dans le contenu. Par bruit nous entendons les mentions « @utilisateur », les hashtags « #hashtag », les smileys et autres chaînes de

caractères non comprises dans le vocabulaire d'un langage. La partie prétraitement des données est donc conséquente et nécessite un nettoyage en plusieurs étapes.

- Nettoyage : à partir d'expressions régulières, nous supprimons les mentions et enlevons le signe « # » ainsi que tout autre symbole n'étant pas un caractère de ponctuation nécessaire à la langue. Au-delà des caractères, certains mots n'apportent aucun intérêt à l'analyse par exemple : « de », « avec », « car ». Il est conseillé de les enlever en utilisant une liste de « Stop Words ».
- Normalisation : dans le cadre d'un modèle dit « Bag of Words » où nous n'accordons pas d'importance à l'ordre dans lequel sont placés les mots dans les phrases, il est fondamental de normaliser les mots possédant la même racine. Dans des langues à déclinaisons telles que l'ukrainien et le russe, cette notion est d'autant plus importante que les mots peuvent fortement varier selon leur objectif dans la phrase. Il existe deux processus de normalisation, le « stemming » et la « semmatization », fondés sur deux approches différentes.
  - stemming : Un algorithme, dont le plus populaire est l'algorithme de Porter, a pour objectif de couper la fin ou le début d'un mot en fonction de sa catégorie grammaticale.
  - lemmatization : Combinaison d'un dictionnaire de vocabulaire avec une analyse morphologique des mots pour en identifier la racine. Le résultat est donc beaucoup plus propre que pour le « stemming », car les mots en sortie conservent un sens et l'erreur est minimisée.

Une fois la mise en qualité faite, pour illustrer la pertinence de la méthode DETEVEN, nous avons calculé, pour chacune des villes et pour chaque jour, le pourcentage d'augmentation de mention du toponyme par rapport à la moyenne du nombre de mentions totales des sept jours précédents. Cela permet de révéler des signaux faibles dans le flux qui seraient inobservables autrement. En effet le flux d'un réseau social comme Twitter privilégie les faits à forte volumétrie.

Si l'on observe le mois d'avril 2014, plus particulièrement la période du 25 au 30 avril, on constate les éléments suivants :

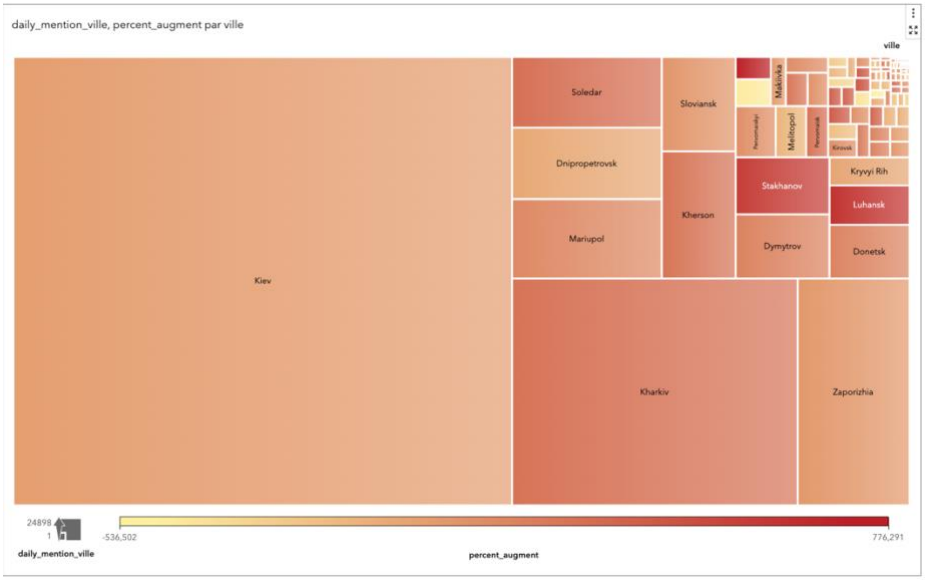


Figure 8 : Vue des tweets du 25 au 30 avril 2014

Si l'on se limite à prendre en compte uniquement la volumétrie, on constate que les plus grosses villes telles que Kiev (24889 mentions sur la période) et Kharkiv (7213 mentions sur la période) monopolisent le flux, voir figure 8.

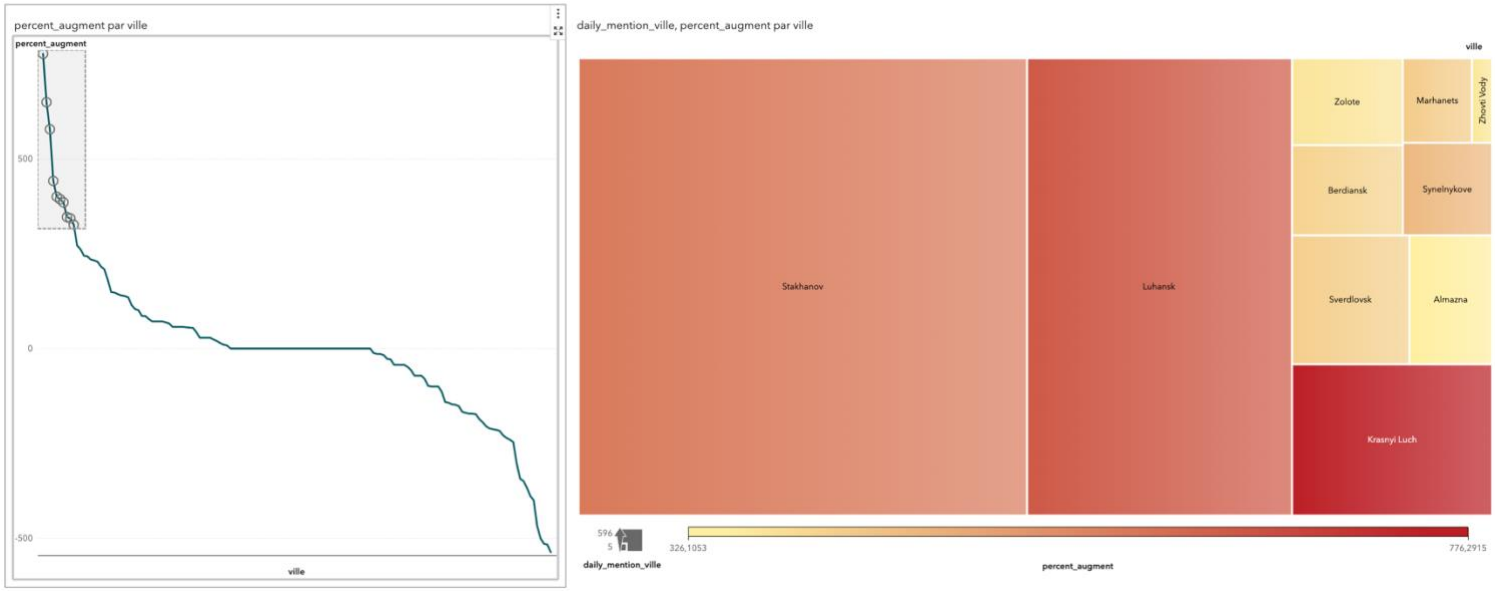


Figure 9a : Vue DETEVEN des tweets du 25 au 30 avril 2014

Si l'on applique la méthode DETEVEN et que sur la même période que précédemment on filtre en prenant les 10 villes ayant connu plus de 300% d'augmentation alors on rend visibles des

villes telles que Stakhanov (596 mentions), Luhansk (352 mentions) et surtout Krasnyi Luch (88). Or, si ces toponymes ont connu une si forte augmentation, c'est parce que des évènements y ont eu lieu. Il s'agit même d'un point tournant dans le conflit. La République populaire de Lougansk est proclamée le 27 avril 2014 et les premières villes à la rejoindre sont Stakhanov et Krasnyi Luch. Elle inscrit le conflit dans une autre dimension en rejoignant la République Populaire de Donetsk proclamée le 7 avril 2014, voir figure 9.

La détection par progression de mention de toponyme permet de ne traiter qu'une infirme partie d'un flux, pour lequel on ne cible qu'une catégorie de mot. Elle est rapide et peut se faire en rétrospectif comme en détection de nouveauté sur de très grands volumes instantanément, près de 10 millions de tweets dans notre cas.

Cette détection peut être représentée visuellement par un graphe en mosaïque (figures 8 et 9) ou par une représentation cartographique. La figure 9b montre des toponymes anormalement présent en décembre 2013 au moment où démarrent les manifestations de masse de Maidan, la ville de Pervomaisk. La figure 9c montre en revanche une multitude de villes de l'est de l'Ukraine anomarlement présente dans le flux au moment des premiers affrontements armés entre les forces ukrainiennes et les séparatistes.

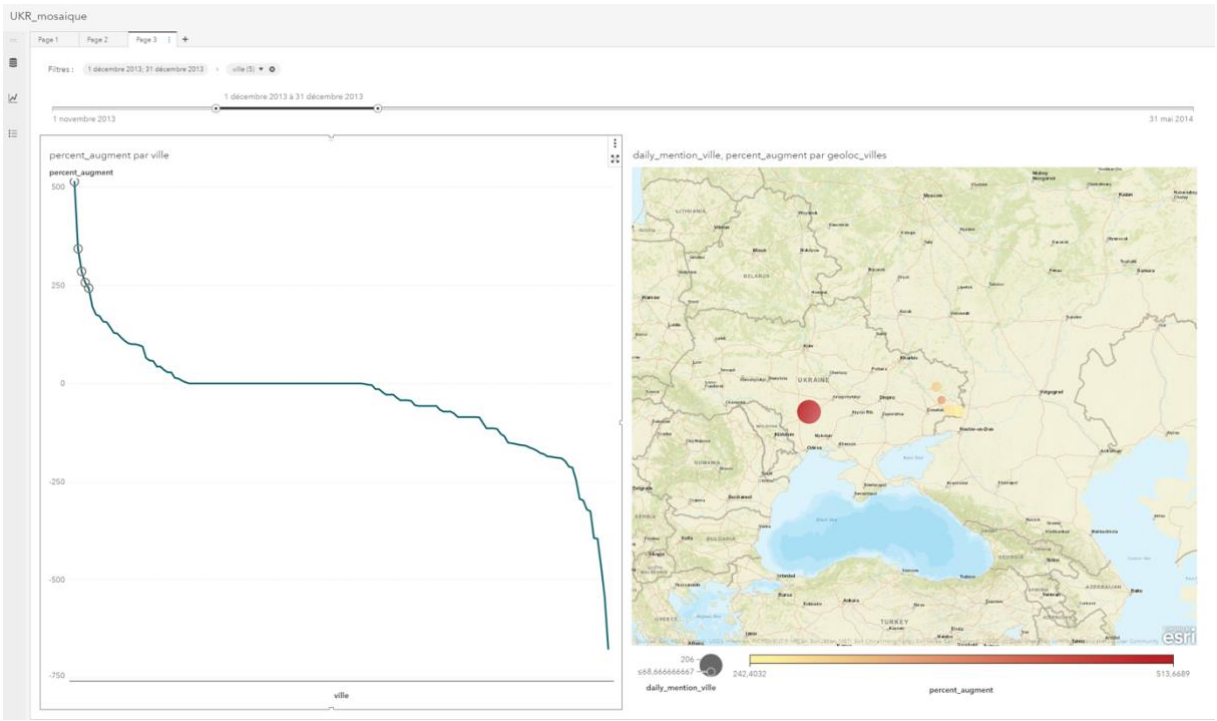


Figure 9b : détection de mentions anormales de toponymes en décembre 2013

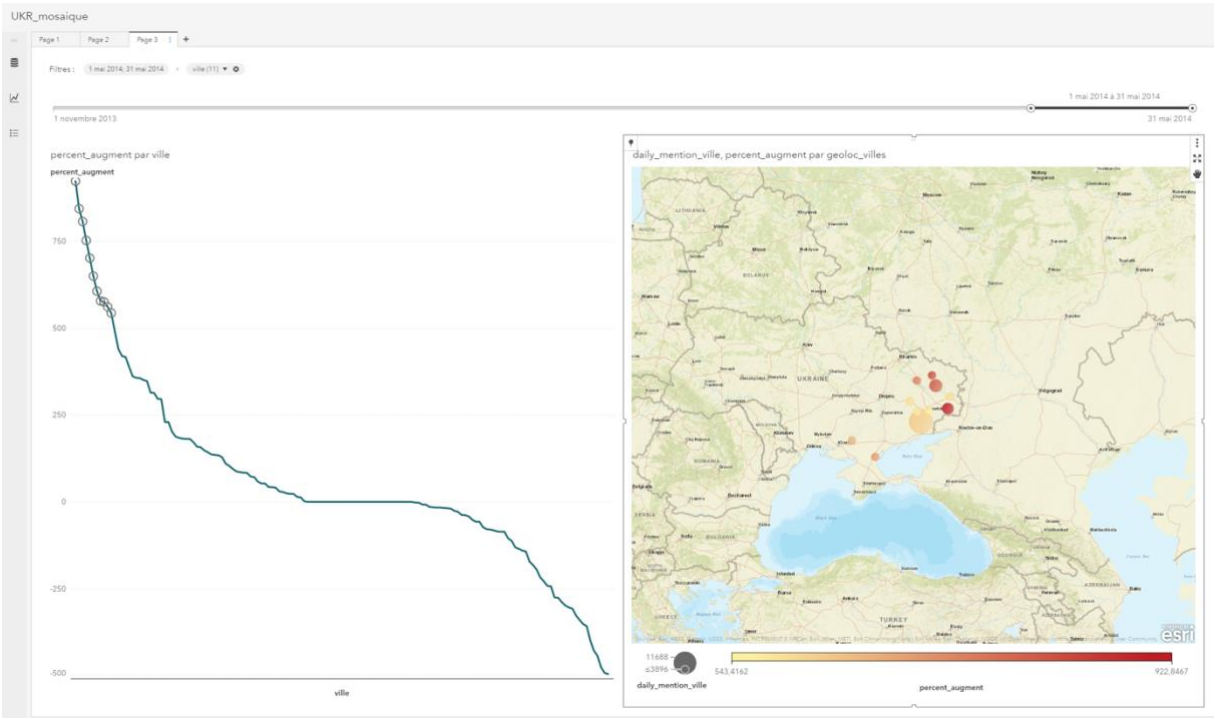


Figure 9c : détection de mentions anormales de toponymes en mai 2014

Une fois les lieux de l'évènement détectés, la sélection automatique de contenu d'intérêt peut se faire également en reconnaissance de concept au moyen d'un dictionnaire ou d'une ontologie hiérarchisant les concepts en fonction de la gravité ou de la valeur d'un mot dans un sujet donné. Cette méthode nécessite une connaissance poussée du sujet surveillé et l'entretien des bases conceptuelles. Une autre approche est la détection des variations dans une zone géographique déterminée telle que :

- l'augmentation subite de la volumétrie globale d'émissions dans une zone donnée ;
- l'augmentation subite de la fréquence de diffusion moyenne par émetteur dans une zone donnée ;
- la concentration thématique ;
- la détection de thèmes émergeants.

L'approche que nous proposons est celle de la détection de concentration thématique non supervisée. Dans un flux de données textuelles tel que Twitter, à un instant donné l'ensemble des sujets de discussion portent une certaine variété sémantique, lors d'un évènement crisogène la concentration thématique permet de détecter l'évènement, voire d'identifier les signaux faibles sans recourir à un dictionnaire.

4.5. Conclusion

Les médias sociaux ne se prêtent pas aux mêmes processus de détection d'évènement que les médias traditionnels. Ils se distinguent notamment par le volume, la variété, la célérité et le caractère éphémère de l'information. De plus, le fait que le contenu soit généré par les utilisateurs implique qu'il y a un fort mélange de genres d'informations diffusées rendant compliquée la détection d'évènement dans le flux. Autre distinction majeure, le format de données permet de travailler sur les caractéristiques du contenant et pas seulement sur celle du contenu. En effet les métadonnées fournissent de nombreuses indications sur l'entité émettrice et sur la portion du réseau sur lequel le contenu est diffusé. Ainsi le flux doit être traité avec une certaine capacité technique pour que le modèle de données puisse prendre en compte l'ensemble des variables d'un tweet par exemple. Enfin la façon de recueillir les données est particulière parce qu'elles sont la propriété des plateformes et sont mises à disposition au moyen d'API dont le taux d'échantillonnage n'est pas révélé.

La détection d'évènement est d'une importance capitale dans des situations de crise telles que les catastrophes naturelles et les conflits. Ces situations correspondent à des pics d'activité des médias sociaux faisant de ces derniers une source d'intérêt pour la détection d'évènement. Malgré les différences avec les médias traditionnels, de nombreuses études ont repris des méthodes en vigueur avant la création des médias sociaux pour effectuer de la détection d'évènement. Elles obtiennent des résultats variables avec une nette avance des études qui prennent en compte les spécificités de médias sociaux. Les recherches d'évènement sont effectuées par détection rétrospective ou par détection de nouveauté. Les objectifs de la détection sont de détecter le plus tôt possible, le plus précisément possible, et de caractériser et catégoriser l'évènement.

La précision correspond au nombre d'évènements pertinents détectés par rapport au nombre total d'évènements détectés, tandis que le rappel correspond au nombre d'évènements pertinents détectés par rapport au nombre total d'évènements pertinents qui existent dans les flux de données. Pour la détection rétrospective, le rappel est généralement difficile à calculer pour des ensembles de données volumineux et bruyants, car l'énumération manuelle de tous les évènements pertinents existant dans un flux Twitter donné est chronophage pour les petits ensembles et est quasiment impossible pour les plus grands.

Chaque algorithme à une finalité : la combinaison d'algorithme est une approche. L'approche que nous avons choisie est l'approche par la notion de lieu : Deteven, pour identifier des évènements (un ensemble de faits), les acteurs, leurs discours. En situation de crise, au-delà des métadonnées techniques de la géolocalisation, des fuseaux horaires, des langues vernaculaires, il s'agit de gens qui rapportent des faits qui les marquent et qu'ils relient à un lieu. Nous souhaitons détecter les évènements émergents au tout début, quand ils ont un impact mineur sur les autres faits. Pour cela nous avons déterminé qu'une détection par mention de toponymes rapportée à la moyenne des jours précédents permet d'identifier les lieux et par extension les évènements.

5. Chapitre 5 : Mise en œuvre de la plateforme sur le conflit ukrainien

5.1. Introduction

L'Ukraine, entre décembre 2013 et juin 2014 a connu plusieurs phases propres à l'identification des phénomènes recherchés. Le pays a traversé toutes les étapes de la contestation passant successivement d'un calme apparent à des manifestations antigouvernementales limitées, à une répression violente, suivie de manifestations massives, qui ont dégénéré en émeutes et rébellion entraînant une révolution, la chute d'un gouvernement, la perte d'une région au profit d'une puissance étrangère, l'auto proclamation de deux républiques autonomes séparatistes aboutissant en une guerre civile. En moins de 6 mois …

Malgré une pénétration d'internet modeste et une utilisation initiale partielle des médias sociaux, leur développement a été sans précédent pendant le conflit. Outils de démocratisation pour les uns et arme de guerres hybrides pour d'autres, les médias sociaux partagent les chercheurs quant à leur rôle dans les mouvements sociaux. Nos travaux illustreront les particularités de l'essor et de l'utilisation de Twitter dans le conflit ukrainien au vu de la place singulière que ce média social occidental a tenu dans ce conflit d'Europe orientale. Plus particulièrement, nous poserons les bases historiques du conflit et en détailleront les phases. Puis nous illustrerons des opérations de guerre hybride sur les médias sociaux.

5.2. La chronologie des évènements

En novembre 2013 l'Ukraine est au bord de la révolution sans que personne n'ait pu le prédire. Les acteurs politiques sont, le gouvernement Yanoukovitch, les partis d'opposition traditionnels (Batkivshchina) et nouveaux (Svoboda, Oudar), le peuple ukrainien. A l'occasion d'un refus de signer un traité de coopération par le gouvernement, le peuple a saisi l'opportunité d'exprimer ses revendications au travers d'un répertoire d'actions collectives à la fois éprouvé (manifestations de masse, occupation de lieux symboliques) et innovant (cortège automobile, camp cosaque). L'ensemble des parties prenantes avaient des points de vue polarisés tant sur l'alignement Est/Ouest que sur l'avenir social et économique du pays. La prolongation de l'effort de contestation et sa violente répression entrainent un mouvement social puis une révolution. Le transfert effectif du pouvoir aux mains d'une opposition hétérogène unifiée dans une coalition d'opportunité est alors fut considéré comme un coup d'état par la partie pro-russe de la population. Cette dernière, à la suite de l'annexion de la Crimée dans les régions de l'Est du pays, le Donbass, décide de faire sécession au travers de deux républiques autoproclamées, la République Populaire de Donetsk et la République Populaire de Lougansk. Pourtant de nombreux signes avant-coureurs existaient. Après-tout le pays avait connu une pseudo-révolution appelée Révolution Orange moins de 10 années auparavant.

Les élections de 2004 avaient opposé un candidat soutenu par la Russie et premier-ministre d'alors (Viktor Yanoukovitch), contre un candidat pro-occidental (Viktor Yushchenko). Le second tour ayant été entaché de très nombreuses irrégularités, des manifestations de masse avaient abouti à l'annulation du second tour et la victoire du candidat pro-occidental au nouveau second tour, évènement appelés Révolution Orange. Les évènements de 2004 n'ont pas eu d'effet durables car les motifs de participation aux rassemblements de masse se sont révélés être des raisons individuelles et non-collectives, la somme de toutes les volontés ne fait pas une union. Il s'agissait d'une coalition temporaire unie principalement par son opposition au régime en place qui ne pouvait survivre à ses forces centrifuges intrinsèques plus précisément aux « *factions avides de pouvoir* » la composant (Beissinger, 2011).

Au résultat, 6 années plus tard, ce même candidat contre lequel la nation s'était révoltée, Viktor Yanoukovitch, remporte l'élection présidentielle de 2010 grâce à un très fort soutien dans les régions orientales traditionnellement enclines à favoriser une plus grande proximité avec la Russie, (voir figure 10). Son pouvoir est renforcé par les élections parlementaires de 2012 qui

donnent une majorité absolue à son parti (voir figure 11). Ce dernier mettra progressivement en place un régime présidentiel donnant une toute-puissance au président.

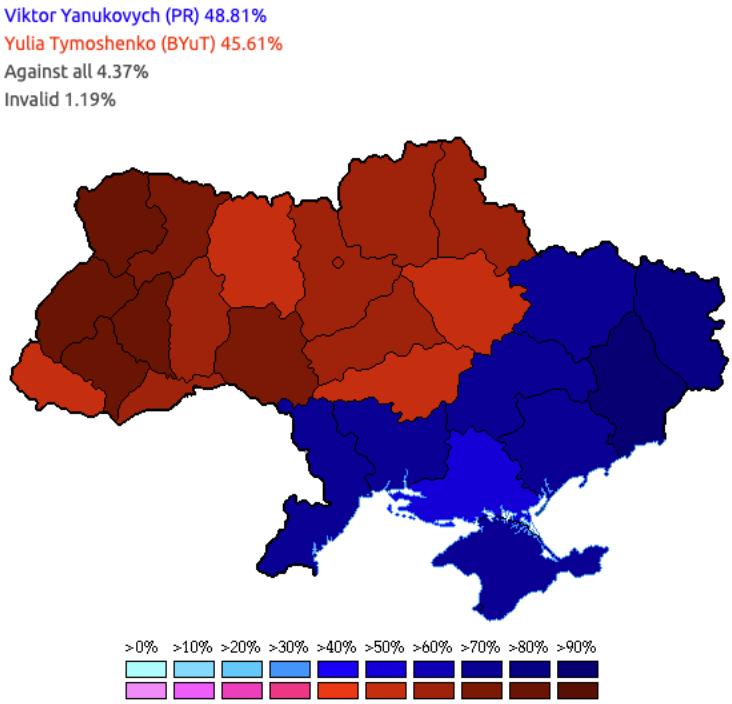


Figure 10 : Carte des résultats des élections présidentielles de 2010

(https://welections.wordpress.com/2010/02/09/ukraine-2010-runoff/)

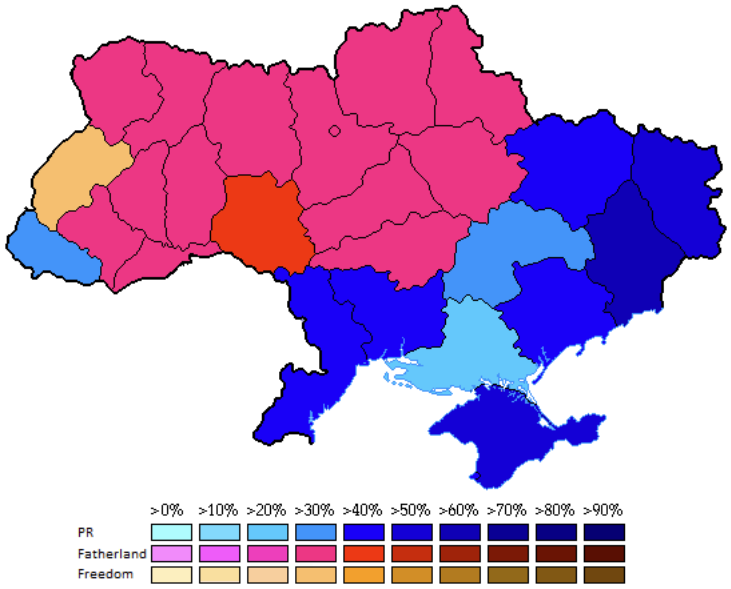


Figure 11 : Carte des résultats des élections parlementaires de 2012

(https://welections.wordpress.com/2012/11/04/ukraine-2012/)

Ces cartes de résultats électoraux caractérisent le clivage du pays qui se révèle également sous d'autres formes. Dans leur étude de 2014, le PEW Research Center met en évidence les facteurs d'unité et de division du pays.

La division géopolitique est relativement marquée et donne l'avantage d'une affiliation à l'Europe pour 43% de la population et à la Russie pour 18%, quand 27% estime qu'il faut avoir des relations équilibrées avec les deux. Ainsi, si 93% de la population de l'Ouest est favorable à l'unité du pays, 70% de la population de l'Est l'est également. La sécession vers la Russie n'est soutenue que par 27% des personnes de l'Est ne parlant que russe. (Pew Research Center, 2014).

A ce titre, le clivage linguistique est à relativiser, 54% de la population estime que l'Ukrainien et le Russe devraient être des langues officielles alors que 41% estime que seul l'Ukrainien devrait avoir ce statut (Pew research Center, ibid.). Nous verrons ultérieurement que le statut des langues sera un des facteurs renforçant la volonté sécessionniste des républiques auto-proclamées. Le clivage linguistique « *suscitant davantage la polémique à l'étranger qu'en Ukraine* » n'est qu'une illusion, 90 % des Ukrainiens comprennent les deux langues. Il n'y a pas de frontière linguistique. (De Suremain, 2014).

Enfin, le dernier clivage à prendre en compte est la différence d'âge entre les membres du parti au pouvoir et les partis de l'opposition, en particulier dans les évènements qui vont suivre et leur lien avec les nouvelles technologies de l'information et de la communication (NTIC). Le parti des régions (au pouvoir) à une moyenne d'âge de 50 ans quand par exemple les partis Svoboda ou Udar est de 43 ans.

L'ensemble de ces clivages renforcés par les malversations constantes, les désillusions de 2004 et l'imminence des élections de 2015 rendent le pays particulièrement instable. « *Plus Yanoukovitch s'éloignera des normes démocratiques afin de renforcer son pouvoir alors qu'il se prépare à être réélu en 2015, plus il est probable que les jeunes gens conduiront de nouveau des personnes dans les rues en signe de protestation pour enfin réaliser leur destin en tant qu'agents de changement.* » (Diuk, 2013). Il est donc nécessaire d'inscrire la crise ukrainienne de 2013-2014 dans la continuité de ces évènements et de prendre en compte les différents clivages du pays pour comprendre la crise ukrainienne de 2013 à 2014.

5.2.1. Phase 1 : les manifestations 22 novembre – 16 janvier

Les manifestations ont commencé à Kiev, la capitale de l'Ukraine, dans la nuit du 21 au 22 novembre 2013. Cette fois-ci, elles n'ont pas été provoquées par des "élections volées" comme en 2004, mais par le refus du président Yanoukovitch de signer un accord de coopération avec l'Union européenne (UE). Le président a pris cette décision sans référendum et l'a fait valider par un parlement acquis à sa cause. Cette décision s'inscrivait dans un contexte économique difficile pour le pays et révélait si besoin était l'influence grandissante de la Russie dans la région. Cette énième décision unilatérale en désaccord avec les aspirations d'une grande partie de la population notamment les jeunes et les classes moyennes a initié les premières manifestations dont Yanoukovitch ne pouvait ignorer la dangerosité du souvenir de son accès au pouvoir barré par la rue en 2004.

Au début, environ 2000 personnes se sont rassemblées puis des centaines de milliers, sur ce qui deviendra le site emblématique de la contestation : la place principale de Kiev, Maidan (place) Nezalezhnosti (de l'Indépendance) qui donnera son nom au principal mouvement de contestation : EuroMaidan dont la première occurrence sera un hashtag sur Twitter, …

Les manifestations ont duré tout le temps du sommet de Vilnius (28-29 novembre 2013) auquel participait Yanoukovitch et durant lequel il aurait dû signer l'accord de coopération. Les premières confrontations avec les forces de l'ordre (29-30 novembre) ont commencé au moment où les manifestants, dans une réminiscence du répertoire d'actions collectives employé en 2004, ont mis en place un camp pour pouvoir tenir la place dans la durée. Ce camp était une référence à la « sich » cosaque, unité militaire composée de centuries « sotnia ». Au cours de cette période, les stratégies d'opposition violente n'ont été utilisées que sporadiquement et de manière non systémique. A ce stade, la plupart des manifestants étaient représentés par la jeune génération. Ils organisèrent une série de processions dans les rues et construisirent une ville de tentes dans le centre de Kiev. La police eu recours à la force pour disperser les manifestants les 30 novembre et 11 décembre 2013. (Oleinik et Strelkova, 2014).

5.2.2. Phase 2 : les manifestations de masse et leur répression 16 janvier – 16 février

Sur la période janvier-février 2014, les affrontements physiques avec la police et les pillages sont devenus prédominants. En outre, le nombre de manifestants a commencé à augmenter à mesure que des membres des générations plus âgées rejoignaient leurs rangs. Au plus fort des

manifestations de décembre 2013, plus d'un million d'Ukrainiens ont pris part à des processions dans les rues de Kiev. Le répertoire des actions de protestation en Ukraine est le résultat d'une recherche ouverte de stratégies modulaires ayant une affinité sélective avec les institutions traditionnelles et une capacité à s'adapter aux nouvelles conditions. Dès le dimanche 1er Décembre, plus de 500 000 personnes se sont rassemblées sur Maidan selon la tradition slave du « Veche » : rassemblement populaire. Ces « Veche » sont planifiés tous les dimanches et sont organisés par les partis d'opposition. Lors du « Veche » du 8 décembre la statue de Lénine sera décapitée et le pavillon des nationalistes ukrainiens du parti Svoboda flotte sur son piédestal. Chaque dimanche de décembre et de janvier réunira plusieurs centaines de millier de personnes sur la place. Les quartiers des institutions gouvernementales situés à proximité seront régulièrement barricadés par les manifestants, la plupart des affrontements avec les forces de l'ordre et les organisations pro-gouvernementales (Antimaidan) se dérouleront autour de ces barricades. Durant tout le mois de décembre, plusieurs violentes confrontations ont lieu entre les manifestants et les forces de l'ordre. Comme annoncé par de nombreux observateurs du mouvement : « *Ianoukovitch aura probablement recours à la coercition, à des moyens extrajudiciaires et à d'autres tactiques pour faire pencher la balance en sa faveur et assurer sa réélection, menaçant ainsi une nouvelle érosion des normes démocratiques* » (Clapper, 2014). C'est ce qui arrive quand le gouvernement fait passer des lois particulièrement répressives le 16 janvier 2014. Parmi elles, les forces de l'ordre obtiennent le droit de géolocaliser les participants aux manifestations au moyen de leur téléphones portables afin de les menacer d'une prochaine arrestation (Hooton, 2014), voir figure 12.

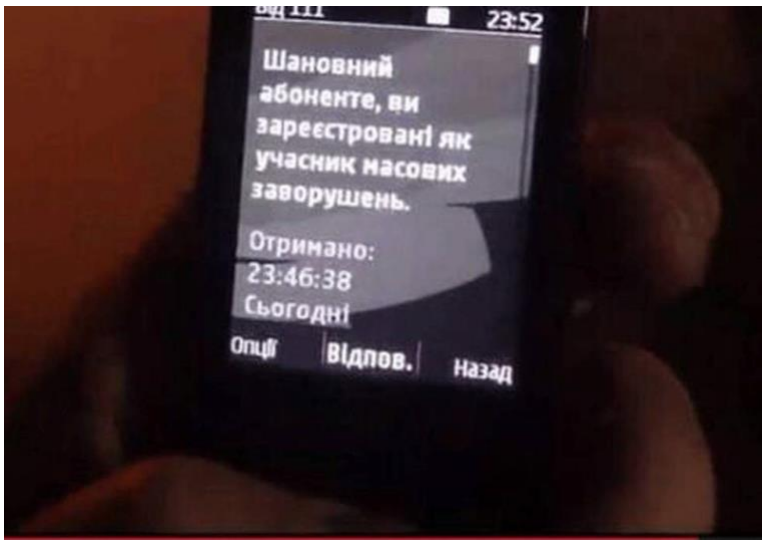


Figure 12 : Photo extraite du compte twitter de Radio Svoboda (compte fermé depuis) le 21 janvier 2014

Traduction de la figure 12 : Cher abonné, vous êtes enregistré en tant que participant à une perturbation de masse.

Ces mesures comprennent également la limitation de la liberté d'expression, l'interdiction de se rassembler à plus de 5 personnes, des jours de prisons et des amendes pour toute forme de participation aux manifestations, etc. La déclaration de l'illégalité des actions du répertoire précédent et l'augmentation de la répression provoquent une rupture (Gomza, 2014). Devant cet acharnement judiciaire, les manifestants redoublent d'effort et les affrontements deviennent plus violent et les premiers morts sont à déplorer. Devant la détermination des manifestant, le 28 janvier le gouvernement démissionne, et le parlement révoque les lois anti-manifestation. Le lendemain une proposition d'amnistie est envoyée aux leaders de l'opposition qui la rejettent. Leur exigence est maintenant le départ du président et des élections anticipées.

5.2.3.27Phase 3 : la révolution

Il s'agit du point où la situation devient révolutionnaire selon les critères de Tilly dans Régimes et Répertoire (Tilly, 2006), pour qui une révolution est le transfert forcé du pouvoir sur un État au cours duquel au moins deux blocs distincts expriment avoir des revendications incompatibles pour contrôler l'État. Les éléments suivants sont alors observables :

- des prétendants ou des coalitions de prétendants poussent des revendications concurrentes exclusives sur le contrôle de l'État ou de certains de ses éléments: processus de mobilisation.
- l'engagement vis-à-vis de ces revendications d'un segment significatif de la population: mobilisation plus diffusion
- l'incapacité ou le refus des dirigeants de réprimer la coalition alternative et / ou de s'en tenir à ses revendications: interaction / défections des sujets soumis au régime par les membres du régime, acquisition de la force armée par des coalitions révolutionnaires neutralisant ou par le contrôle par la force du contrôle des forces armées par l'appareil du régime transfert de la coalition révolutionnaire du pouvoir d'État à la nouvelle coalition au pouvoir.

Tout bascule entre le 17 et le 21 février dans ce que l'on décrirait comme des « moments de folies » « *nécessaires à la transformation politique des sociétés, car ils sont la source de nouveaux acteurs et publics et de la force nécessaire pour percer le fardeau de la convention.* » (Zolberg, op. cit.). En effet, devant les prérequis et ultimatum successifs du gouvernement

comme préalables à toutes négociations, certains éléments parmi les plus radicaux de l'opposition, le parti Praviy Sector appellent les citoyens à la résistance armée. Le gouvernement espère suffisamment de débordements pour justifier un état d'urgence et ainsi avoir la capacité à engager des unités militaires et paramilitaires en plus de troupes anti-émeutes (Berkut). Il n'en aura pas le temps, le déchainement de violence fera 80 morts dont 60 pour la seule journée du 20 février dont une majorité par tir de sniper. (Scheide et Schmidt, 2014). Le 22 février Yanoukovich fuit le pays, le parlement vote un retour à la constitution de 2004 limitant les pouvoirs présidentiels.

5.2.4. Phase 4 : Annexion de la Crimée par la Russie

Dans le but de satisfaire chacune des composantes très diverses de l'opposition, une série de décisions contestables vont être mises en œuvre le nouveau gouvernement. Le Parlement vote l'interdiction du russe en tant que deuxième langue officielle, provoquant une vague de colère dans les régions russophones. Le vote est ensuite annulé, mais le mal est fait. L'unité de police d'élite, le Berkut, désignée seule responsable de la mort de manifestants, est dissoute. (BBC, 2014). Ces deux décisions auront pour conséquence d'inquiéter les régions pro-russes de l'Est et de leur fournir des éléments armés et formés au combat qui viennent ainsi d'être déclarés traitres à la nation … Les 27 et 28 février, des soldats sans insignes surnommés « petits hommes verts » prennent possession des principaux bâtiments administratifs et militaires de Crimée. Le 6 mars : les dirigeants pro-russes de la Crimée votent pour l'adhésion à la Russie et organisent le référendum du 16 mars, aggravant ainsi la crise (Reuters, 2014).

Cette phase n'est pas dans le périmètre de nos recherches du fait de l'absence de situation conflictuelle. En effet l'opération russe et le soutien avéré de la population locale a eu un effet de saisissement des quelques forces ukrainiennes sur la presqu'île.

5.2.5. Phase 5 : Sécession des républiques auto-proclamées de Donetsk et de Lougansk et guerre civile (avril- septembre 2014)

Le 6 avril, des rebelles pro-russes s'emparent de bâtiments gouvernementaux dans les villes de Donetsk, Louhansk et Kharkiv, à l'est du pays, appelant à un référendum sur l'indépendance et à la revendication d'une république indépendante. Les autorités ukrainiennes ont repris le contrôle des bâtiments de Kharkiv le 8 avril après le lancement d'une « opération

antiterroriste », mais les autres villes restent incontrôlables. (Independant, 2014). Progressivement la majeure partie des régions de Donetsk et de Lougansk basculeront dans la rébellion contre le nouveau gouvernement issu de la révolution.

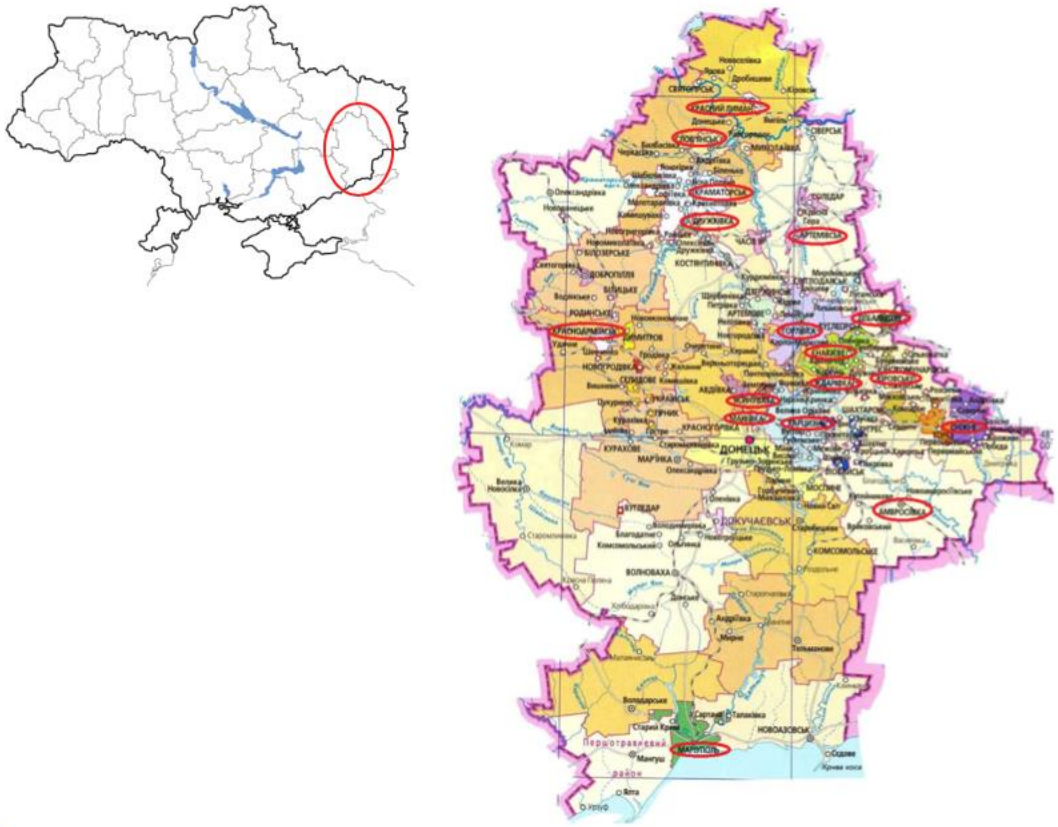


Figure 13 : Carte des villes revendiquées comme prises par les séparatistes de la République Populaire de Donetsk, en avril 2014

Un premier tournant dans la guerre civile sera la désignation des séparatistes comme étant des terroristes par le gouvernement de Kiev. Dès lors rien n'empêche le lancement d'une opération anti-terroriste le 13 avril depuis l'aérodrome de Kramatorsk avec comme premier objectif la reconquête de la ville de Slaviansk bastion de la défense des séparatistes. Les combats dureront jusqu'au traité de Minsk (5 septembre 2014) qui, s'il n'empêche pas le nombre de victimes d'augmenter encore à ce jour, restreint les manœuvres d'envergure des belligérants. Ce traité sera complété par une deuxième version en février 2015.

5.3. Guerre hybride et préparation des données

5.3.1. Prétraitements : twitterbots, influence et retweet

Avant de pouvoir étudier les tweets collectés un certain nombre de prétraitements doivent être réalisés pour limiter les biais d'analyse. Un des premiers traitements a effectué est d'identifier et d'isoler les tweets en provenance manifeste d'un twitter bot. Plusieurs méthodes peuvent être employées dont celles portant sur les caractéristiques du profil et celles portant sur les caractéristiques du comportement. Dans les éléments du profil il est possible d'identifier les comptes avec une date de création relativement récente, les noms de compte contenant des nombres ce qui pourrait indiquer la génération automatique de noms. L'absence de biographie ou de photo peut également être un indicateur. Dans les éléments de comportements, il est possible d'identifier les comptes qui ne font que retweeter et ne diffuse aucun contenu original, de noter si la fréquence de tweet du compte est supérieure à celle d'un utilisateur humain ou d'identifier les comptes diffusant énormément de tweets mais ne comptant que quelques abonnés. Par ailleurs, les comptes de bots peuvent tweeter le même contenu que d'autres utilisateurs à peu près au même moment sans qu'il s'agisse d'un retweet. Enfin, de courtes réponses à d'autres tweets peuvent également indiquer un comportement automatisé. L'identification des bots sur les réseaux sociaux est d'une importance capitale non seulement pour apurer les données de recherche, mais parce qu'il s'agit d'un puissant outil de manipulation des masses. Ainsi la DARPA, agence du département de la Défense des États-Unis chargée de la recherche et développement des nouvelles technologies destinées à un usage militaire a lancé un challenge en 2015 pour identifier les bots (Subrahmanian, 2016).

Dans notre jeu de donnée nous avons employé deux méthodes : la détection de la diffusion en réseau, et la modélisation de comportement.

Dans la méthode de diffusion en réseau, le but est de détecter les botnets comme un réseau de compte diffusant de manière massive et instantanée le même contenu sur le média social (Twitter, FB, ...). Ici il ne s'agit pas de détecter, sur la base de l'activité d'un seul compte, si ce compte est réel ou non ; mais plutôt de détecter du contenu diffusé massivement afin de caractériser l'activité de ces comptes ayant ce comportement. Dans notre jeu de donnée sur l'Ukraine certains comptes publiaient exactement le même message sur Twitter sans que ce tweet ne soit estampillé comme étant un retweet. En prenant le jeu de données complet, basé

sur une collecte par mot clés et localisation, nous avons cherché à identifier les messages Twitter supérieurs à 5 mots qui apparaissent plusieurs fois, et publiés par des comptes distincts, dans une période de temps inférieure à 2-3 jours. Le filtre sur la période de temps n'est pas nécessaire au début, et peut-être placé plus tard pour une analyse plus en détail de la diffusion du message.

Dans un second temps, nous avons agrégé les messages twitter non pas par contenu exact, mais par contenu semblable via logique floue, en calculant une distance entre chaque message, basée sur le nombre de mots/lettres en commun/différent. Cela nous a certes permis d'aller plus loin que la correspondance stricte, mais en générant plus de bruit.

Autre approche employée dans notre jeu de donnée nous avons regroupé les tweetos diffusant les mêmes URL. Cette détection de diffusion artificielle de contenu, que ce soit des liens vers des articles de presse, des vidéos, ou même d'autres messages sur des réseaux sociaux, permettent de mettre en évidence des réseaux de bot dont le rôle est justement de relayer ces contenus de manière artificielle pour en augmenter la portée. Cela nous permet également de découvrir, au milieu de contenus de peu d'intérêt, des contenus de propagande ou des fake news, dont une des forces est justement la diffusion rapide et incontrôlée. Dans la détection de tels contenus, une des problématiques possibles est également le masquage des adresses URL par Twitter, qui va donner des URL réduites au lieu des véritables URL dans l'optique de réduire le nombre de caractères utilisés. Cette problématique est due à la structure interne du message twitter, limité en termes de nombre de caractère. Cas des contenus médias images/vidéos : ce type de contenu est très utilisé sur les réseaux sociaux, et de plus en plus aujourd'hui. Il peut également servir à détecter des réseaux de botnets, avec la même technique que précédemment. Le critère d'agrégation va donc être que plusieurs comptes vont diffuser le même média sur un temps court. Pour détecter si le média est identique il n’est pas possible de se baser sur l’URL vu que celle-ci est modifiée automatiquement par Twitter. Pour le faire il faut d'utiliser des techniques de hash qui permettent de trouver une "signature" à l'image. Ainsi, deux images strictement identiques auront les mêmes « hash » (signature numérique). Il existe des techniques plus élaborées permettant de faire matcher des images n'étant pas complètement identiques, et pour permettre notamment d'aller au-delà de contre-mesure consistant à changer quelques pixels dans l'image afin d'éviter la détection automatique d'image identique.

La détection des twitter bot, via de la modélisation de comportement : certains bots peuvent être détectés assez simplement grâce à leur activité de publication ; en effet, ils publient des messages toujours aux mêmes heures de la journée, sur une certaine période de temps. Si on a

donc monitoré et récupéré toute leur activité, on découvre très facilement ce pattern en aggrégeant son activité dans le temps à l'heure, à la minute, voire à la seconde.

Dans toutes les statistiques qui vont suivre, nous nous plaçons sur la période de janvier et février 2014.

	verb	body	MIN_of_Posted Time	MAX_of_Posted Time	Etendue_periode	Nb_tweet_identique	COUNT_DISTINCT_of_actor_id
1	post	#СевастопольРоссия В Севастополе послали ко всем чертям Киев!	25FEB14:10:03:12	25FEB14:12:33:57	2:30:45	722	384
2	post	#СевастопольРоссия По предварительной информации Киев уже готов отключить нам свет,воду,связь и вообще полностью блокировать город.	25FEB14:10:02:11	25FEB14:12:33:56	2:31:45	713	396
3	post	#СевастопольРоссия Сейчас все прекрасно понимаю,что фашистский Киев начнёт нас просто убивать за это демократический "бунт"	25FEB14:10:04:46	25FEB14:12:33:56	2:29:10	712	387
4	post	#СевастопольРоссия Также было решено в Киев больше не отправлять налоги.	25FEB14:10:05:08	25FEB14:12:33:41	2:28:33	711	388
5	post	Наймасовіша акція безперервно проходить у Києві. За цей час учасників протесту на площі Незалежності кілька	16JAN14:14:18:04	26FEB14:14:29:50	984:11	418	8
6	post	"Автомобилист" всухую обыграл минское "Динамо"	17JAN14:03:40:14	18JAN14:18:48:20	39:08:06	411	411
7	post	Майдан и власть еще долго будут играть друг с другом в догонялки. - общественник	19JAN14:18:36:41	19FEB14:07:52:32	733:15	405	403
8	post	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:15:14:34	20JAN14:21:56:12	30:41:38	404	404
9	post	Во Львове готовят автопробег "Все на Киев! Имей совесть"	20JAN14:11:26:34	21FEB14:19:24:31	775:57	401	401
10	post	Верховная Рада приняла решение работать без перерыва до окончания кризиса	20FEB14:21:24:33	22FEB14:05:37:33	32:13:00	400	400
11	post	Фанаты киевского "Динамо" выйдут сегодня охотиться на "титушек"	21JAN14:22:41:56	23JAN14:01:53:05	27:11:09	398	397
12	post	Сотни одесситов выстроились на Потемкинской лестнице в живую желто-голубую цепь: "Киев мы с тобой!" (ВИДЕО, ФОТО)	23JAN14:00:10:01	24JAN14:05:25:19	29:15:18	395	394
13	post	Верховная Рада отобрала резиденцию "Межигорье" у Януковича	23FEB14:11:06:03	24FEB14:20:49:34	33:43:31	380	379
14	post	Силовики частично заняли Майдан Незалежности	18FEB14:20:35:08	20FEB14:00:40:03	28:04:55	372	372
15	post	"Беркут" неудачно атаковал Майдан и потерял "множество" бойцов пленными	18FEB14:22:49:35	20FEB14:02:30:11	27:40:36	369	368
16	post	Верховная Рада продолжает увольнять людей Януковича / С должностями попрощались Королевская, Новохатько, Табачник и СБУшник Якименко	24FEB14:16:51:01	25FEB14:23:54:26	31:03:25	366	366
17	post	Литва отмечает День восстановления независимости / В Вильнюсе - огромный флаг, костры и призыв к единению общества	16FEB14:13:03:02	17FEB14:08:16:34	19:13:32	360	360
18	post	Улыбни свой улыбальник и будет тебе счастье :-)	16FEB14:00:26:57	26FEB14:02:01:50	241:34	276	140
19	post	Лига Европы: победа "Днепра", ничья "Шахтера", поражение "Динамо"	21FEB14:00:01:36	26FEB14:21:29:17	141:27	269	171
20	post	Что подарит Киев лучшему диджею планеты?	16JAN14:00:16:44	25FEB14:17:48:53	977:32	267	96
21	post	УЕФА перенес матч "Динамо" с "Валенсией" из Киева на Кипр	19FEB14:15:37:30	26FEB14:22:45:18	175:07	264	166
22	post	Майдан в регионах Украины: обновляется	23FEB14:07:37:42	26FEB14:18:53:00	83:15:18	252	116
23	post	У России две беды: украинский майдан и датский жираф.	16FEB14:06:01:50	25FEB14:05:44:22	215:42	224	220
24	post	Одинаковое счастье - быть победителем или побежденным в битвах любви.	16JAN14:14:31:41	26FEB14:23:58:07	993:26	206	193
25	post	Майдан в Киеве: прямая онлайн видеотрансляция	17JAN14:08:52:00	26FEB14:16:45:00	967:53	203	117
26	post	Самое большое счастье в жизни - это уверенность в том, что тебя любят	16JAN14:00:12:03	26FEB14:23:47:09	1007:35	203	194
27	post	Счастье классиков в том, что они мертвы. Наше и ваше счастье в том, что они мертвы.	16JAN14:01:14:02	26FEB14:21:01:24	1003:47	197	181
28	post	Несчастье никогда не сломает того, кого не обмануло счастье.	16JAN14:05:15:19	26FEB14:22:41:43	1001:26	196	189
29	post	Счастье продает нетерпеливым людям великое множество таких вещей, которые даром отдает терпеливым.	16JAN14:09:22:09	26FEB14:23:47:39	998:25	190	177
30	post	#Євромайдан #Янукович #Автомайдан #Тимошенко #Яценюк #Грушевського #Уряд #Опозиція	16FEB14:00:03:42	24FEB14:03:46:45	195:43	189	146
31	post	Все люди попадают в нашу жизнь не просто так. Одни приносят счастье, а другие опыт и закалённый характер.	16JAN14:04:23:03	26FEB14:20:29:22	1000:06	181	173
32	post	Счастье заключается не во всяком удовольствии, а только в честном и благородном.	16JAN14:02:08:25	26FEB14:20:11:08	1002:02	172	162
33	post	В счастье легко найти друга, в несчастье же в высшей степени трудно.	16JAN14:04:45:37	26FEB14:22:40:53	1001:55	167	159
34	post	В счастье не следует быть чрезмерно самоуверенным, а в беде не следует терять уверенность.	16JAN14:07:14:03	26FEB14:23:18:14	1000:04	159	146
35	post	Счастье редко сопутствует уходящим: оно радушно привечает и равнодушно провожает.	16JAN14:04:30:49	26FEB14:21:45:05	1001:14	155	151
36	post	Истинное счастье для нас – вещь отрицательная: она состоит в отсутствии бедствий.	16JAN14:08:10:38	26FEB14:22:48:07	998:37	146	141
37	post	Хочу, чтобы судьба взяла меня за волосы и прямо мордой - в счастье, в счастье, в счастье!	16JAN14:05:18:15	26FEB14:22:49:46	1001:31	144	105
38	post	Декларация Независимости США написана на бумаге из конопли.	17JAN14:06:00:35	26FEB14:18:17:04	972:16	142	12
39	post	Разбитая посуда приносит счастье, но только археологам.	16JAN14:14:36:05	26FEB14:21:24:50	990:48	142	138
40	post	Майдан выдвинул Яценюка в премьеры Украины	26FEB14:19:09:53	26FEB14:23:18:13	4:08:20	139	139
41	post	Счастье обычно приносят и уносят одни и те же люди.	16JAN14:08:27:12	26FEB14:20:58:39	996:31	136	125
42	post	Все люди приносят счастье. Одни своим присутствием, другие - отсутствием.	16JAN14:04:45:40	26FEB14:22:03:52	1001:18	136	119

Figure 14 : Tableau 1, ordonnancement par volume des tweets identiques sans la mention de retweet (masquage volontaire), extrait de la plateforme DETEVEN

Ce tableau nous permet de voir le nombre de fois où un même texte (body) a été tweeté (le texte a été « copié collé ») sans avoir été retweeté. Prenons la première ligne dans la table ci-dessus, on voit que ce post : « #СевастопольРоссия В Севастополе послали ко всем чертям Киев! » au groupe date/heure (GDH) du 25 février 2014, 10 : 03 :12 (MIN of Posted Time) et 12 :33 :57 (MAX of Posted Time) a été tweeté 722 fois (Nb_tweet_identique) par 384 acteurs différents (count_distinct_of_actor_id). Etendue_periode = Max_of_postedTime – Min_of_PostedTime soit en 2 heures, 30 minutes et 45 secondes.

Le plus intéressant est lorsque l'on regarde les lignes 2, 3, 4 et 5 :

#СевастопольРоссия В Севастополе послали ко всем чертям Киев!	25Feb2014 10:03:12	25Feb2014 12:33:57	0:48:06	2:30:45	722
#СевастопольРоссия По предварительной информации Киев уже готов отключить нам свет,воду,связь и вообще полностью блокировать город.	25Feb2014 10:02:11	25Feb2014 12:33:56	0:47:59	2:31:45	713
#СевастопольРоссия Сейчас все прекрасно понимаю,что фашистский Киев начнёт нас просто убивать за это демократический "бунт"	25Feb2014 10:04:46	25Feb2014 12:33:56	0:48:02	2:29:10	712
#СевастопольРоссия Также было решено в Киев больше не отправлять налоги.	25Feb2014 10:05:08	25Feb2014 12:33:41	0:48:49	2:28:33	711

Les textes, particulièrement polarisants, se traduisent comme tels :

- #SebastopolRussie À Sébastopol, on dit à Kiev d'aller au diable !
- #SebastopolRussie Selon des informations préliminaires, Kiev est déjà prête à couper le courant, l'eau, et les communications et, en général, à bloquer complètement la ville.
- #SebastopolRussie Maintenant, je comprends parfaitement que les fascistes de Kiev vont tout simplement nous tuer au nom de cette « rébellion » démocratique
- #SebastopolRussie Il a également été décidé de ne plus envoyer les impôts à Kiev.

Les faits que tous aient été émis le 25 février entre 10:03 et 10:05 entre 711 et 722 fois dans un laps de temps d'environ 2h et 30 minutes par un nombre d'acteurs situé entre 384 et 396 est trop régulier pour être un hasard. Il s'agit très probablement d'un réseau de bots.

En prenant le tweet ligne 8 du tableau de la figure 15, ci-dessous, « Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке » (La rue Grushevskovo sous les gazes lacrymogènes – Les « Berkuts » se préparent à contre-attaquer) on peut détailler les pics intéressants

count_of_postedtime>6

	body	PostedTime	COUNT_of_body	COUNT_of_PostedTime
1	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:15:24:19	404	9
2	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:15:51:04	404	23
3	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:15:51:05	404	45
4	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:15:54:19	404	20
5	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:16:33:04	404	11
6	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:16:34:33	404	7
7	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:16:54:03	404	12
8	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:18:52:03	404	36
9	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:18:52:04	404	7
10	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:18:52:05	404	25
11	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:18:52:06	404	10
12	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:19:55:03	404	10
13	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:21:51:49	404	34
14	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:21:52:04	404	101
15	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:21:52:05	404	24
16	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:21:53:10	404	11
17	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:22:33:48	404	19
18	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:22:35:18	404	9
19	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	19JAN14:22:55:07	404	8
20	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:00:53:03	404	28
21	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:00:53:05	404	12
22	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:00:53:07	404	10
23	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:00:53:08	404	8
24	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:00:53:09	404	10
25	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:00:53:10	404	7
26	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:00:53:11	404	7
27	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:01:35:04	404	8
28	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:03:53:03	404	9
29	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:03:53:06	404	9
30	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:04:55:33	404	9
31	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:06:53:05	404	7
32	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:06:53:19	404	7
33	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:09:53:33	404	23
34	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:09:53:48	404	9
35	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:12:54:03	404	41
36	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:12:54:05	404	40
37	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:12:54:10	404	7
38	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:14:00:48	404	15
39	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:15:54:34	404	81
40	Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке	20JAN14:15:54:49	404	25

Figure 15 : Tableau 2 : Ordonnancement temporel des tweets similaires, extrait de la plateforme DETEVEN

Count_of_body représente le nombre de fois total où le texte « Улица Грушевского в слезоточивом газе - "Беркут" готовится к контратаке » a été tweeté, et count_of_postedtime le nombre de fois où il a été tweeté à cet horaire précis.

Toujours en restant dans notre échantillon janvier/février (1.308.346 tweets), on découvre dans la base 1291 utilisateurs ayant posté au moins une fois plus d'un tweet en moins d'une seconde ...

Voici l'exemple d'un utilisateur assez coutumier du fait :

	actor_id	PostedTime	COUNT_DISTINCT_of_Tweet_id
1	945667194	26FEB14:15:31:11	2
2	945667194	26FEB14:15:30:57	3
3	945667194	26FEB14:15:30:27	4
4	945667194	26FEB14:15:30:03	6
5	945667194	26FEB14:15:29:50	3
6	945667194	26FEB14:15:28:58	17
7	945667194	26FEB14:15:28:57	4
8	945667194	26FEB14:15:27:37	22
9	945667194	26FEB14:15:27:18	2
10	945667194	26FEB14:15:27:10	22
11	945667194	19FEB14:18:49:19	2
12	945667194	19FEB14:18:49:02	2
13	945667194	19FEB14:18:46:46	2
14	945667194	19FEB14:18:46:45	2
15	945667194	19FEB14:18:42:07	4
16	945667194	19FEB14:18:39:12	2
17	945667194	19FEB14:18:39:11	4
18	945667194	19FEB14:18:38:56	2
19	945667194	19FEB14:18:06:38	2
20	945667194	19FEB14:18:04:33	3
21	945667194	19FEB14:18:04:32	2
22	945667194	19FEB14:18:04:24	2
23	945667194	19FEB14:18:00:31	2
24	945667194	19FEB14:18:00:23	2
25	945667194	19FEB14:18:00:22	2
26	945667194	19FEB14:18:00:15	3
27	945667194	19FEB14:17:59:01	3
28	945667194	19FEB14:16:57:18	2
29	945667194	19FEB14:16:57:11	2
30	945667194	19FEB14:16:55:29	2
31	945667194	19FEB14:16:55:28	2
32	945667194	19FEB14:16:55:20	2
33	945667194	19FEB14:16:53:36	3
34	945667194	19FEB14:16:51:44	2
35	945667194	19FEB14:13:29:15	2
36	945667194	19FEB14:13:27:21	2
37	945667194	19FEB14:13:23:15	2
38	945667194	19FEB14:13:20:39	2
39	945667194	19FEB14:13:16:52	2
40	945667194	19FEB14:13:15:50	2
41	945667194	18FEB14:22:45:18	2

Figure 16, tableau 3 : Suivi d'un tweetos diffusant des tweets identiques plusieurs fois par secondes, extrait de la plateforme DETEVEN

Le 26 février, il a posté deux fois 22 tweets en une seconde une première fois à 15 :27 :10 et une seconde fois à 15 :27 :37 et une fois 17 tweets la même seconde. Cet utilisateur est d'autant plus intéressant qu'il poste des messages différents et n'est donc pas a priori détecté comme bot.

5.3.2. La gestion des retweets (RT)

Sur le segment allant du 1 janvier 2014 au 31 mai 2014, il y a eu 8 644 979 émissions dont 5 358 193 tweets et 3 286 786 Retweets sans compter les messages copié/collé. Lorsque l'objectif est d'accéder à des sources primaires ou de travailler sur les signaux faibles, il peut être nécessaire de pondérer les RT de manière à pouvoir distinguer les tweets uniques dans la masse de RT. A une requête donnée il faut pouvoir réduire tous les tweets au tweet d'origine pour voir toutes les opinions et dans un deuxième temps avoir une capacité d'affichage volumétrique des RT par postedTime et location.

L'action de retweeter, faite par un utilisateur véritable (et non par une machine), a du sens et peut être interprétée de différentes façons. La génération de tweet et retweet lors d'un évènement sont des activités complémentaires et de substitution, dans la mesure où pour répondre à un tweet il faut qu'il ait été émis et lorsqu'on retweet on ne peut pas générer d'information nouvelle. A un instant T l'utilisateur doit choisir entre la création d'information et l'interaction sociale (Chierichetti, et al., 2014). « *Retweeter indique non seulement un intérêt pour un message, mais également une confiance dans le message et son auteur et un accord sur le contenu du message. L'inclusion de hashtags renforce le signal d'accord, surtout lorsque les hashtags sont liés à la politique.* » (Metaxas et al., 2015). De plus, le volume de Retweet est un bon indicateur du niveau d'influence d'un utilisateur du réseau. Il existe différents types de retweet, des retweets secs réalisés automatiquement et mot pour mot, jusqu'à des retweets avec mention du nom de la source et modification et/ou ajout de hashtags. La nature des retweets en révèle plus sur l'influence d'une personne que son volume d'abonnés. Ainsi un utilisateur ayant des retweets mentionnant son nom révèle sa capacité à faire relayer de l'information en étant une source légitime quand un utilisateur ayant des mentions de son nom révèlera sa capacité à engager son public. Le volume d'abonnés indique la popularité mais « *les retweets sont générés par la valeur du contenu d'un tweet, tandis que les mentions sont gérées par le nom valeur de l'utilisateur* » (Cha et al. 2015).

Le fait de retweeter peut également relever d'une action délibérée à visée politique : *« d'essayer de rendre le sujet si populaire qu'il apparaisse sur la page "sujets d'actualité" de Twitter et soit ainsi diffusé à un grand nombre d'utilisateurs de Twitter qui pourraient autrement ne pas le rencontrer*. » (Yardi et Boyd, 2010). Dans ce cas le retweet est une forme de système de curation par la foule dans un but précis (Starbird, Palen, op. cit.).

5.4. Twitter une révolution, analyse d'un théâtre d'opération connecté

Globalement l'Ukraine était en 2013 un pays où l'usage d'internet était considéré comme libre (FreedomHouse, 2013) Le taux de pénétration d'Internet en 2014, 34%, le taux le plus faible en Europe qui disposait alors d'une moyenne de 69%. Avec 15 millions d'utilisateurs d'internet, 27% de la population soit (12 millions) utilisent les médias sociaux, taux également parmi les plus faibles d'Europe. Le taux de pénétration de téléphone mobile est de 133% soit un des taux les plus élevés d'Europe (dans le top 10) mais seul 6% des abonnements fournissent un accès à la données (taux le plus faible d'Europe) avec 2,5 millions de personnes ayant une connexion internet mobile générant 4,1 millions d'utilisateurs mensuels actifs sur les réseaux sociaux au travers d'un téléphone portable (WeareSocial, 2014).

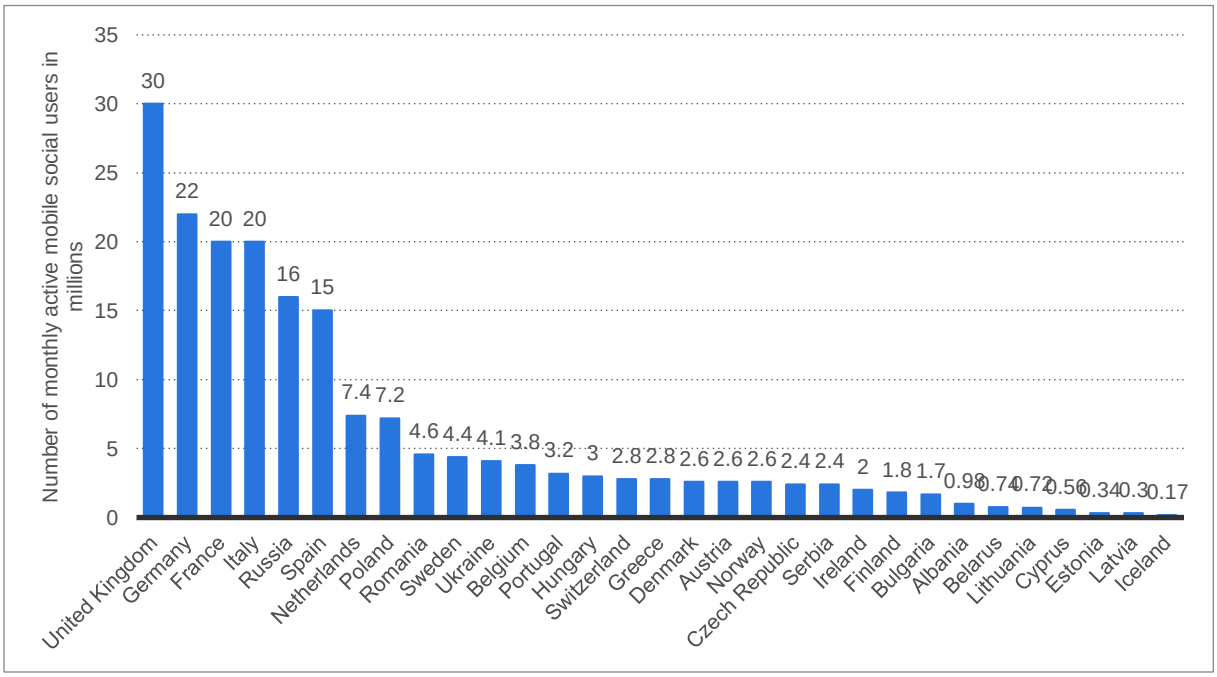


Figure 17, graphique 1 : Moyenne mensuelle du nombre d'utilisateurs actifs de téléphone mobile en millions en Europe en 2014 (Statista, 2014 a)

Le paysage des médias sociaux en Ukraine était très largement dominé par les sites russes :

- VKontakte 27 millions d'utilisateurs,
- Odnoklassniki 11 millions,
- Facebook 3,2 millions
- Twitter 430 000 (Yandex, 2014a).

Tous les médias sociaux ont vu la création de groupe pro et anti Maidan particulièrement polarisés. Deux médias se distinguent, VKontakte de par sa position très largement dominante et Twitter par sa formidable progression durant le conflit.

Vkontakte (VK) est similaire en fonctions à Facebook un utilisateur peut créer un profil (public ou privé) puis commencer “Friender” d'autres utilisateurs. Les utilisateurs de VK peuvent échanger des messages entre eux en privé ou poster/rediffuser des messages et partager publiquement divers contenus multimédias. Ils peuvent également interagir avec un contenu du site Web de VK en « aimant » ou en laissant des commentaires. Les utilisateurs de VK peuvent organiser un groupe public ou privé ou une page de communauté. Au sein des groupes les plus actifs sur VK durant le conflit, deux profils sont caractéristiques du clivage parmi les pro- et les anti- Maidan.

- Un premier groupe pro-russe, à l'origine axé sur l'anti-américanisme. Dès le début de l’année 2014, il a concentré son attention sur le soutien de l'activisme anti-Maidan, y compris le soutien de deux républiques autoproclamées - Donetsk et Lougansk.
- Un second groupe a soutenu les activités anti-Maidan dans le Donbass, la région de l'est de l'Ukraine. Son objectif était de recruter des volontaires, du personnel militaire et d’autres professionnels pour la cause de la République. Le groupe était également un lieu de partage des nouvelles récentes sur la République et des actions de sa milice.
- Un premier groupe pro-Maidan ukrainien avait pour objectif général de réunir, de coordonner les activités de la société civile en Ukraine et de relancer le système de gouvernement et contribuer à l'intégration européenne.
- Un second groupe pro-Maidan s'est formé début avril pour soutenir l'opération antiterroriste menée par le gouvernement ukrainien

Au vu des contenus diffusés sur ces groupes, une première distinction flagrante était à faire entre les évènements de 2004 et ceux de 2014 : « *beaucoup de personnes dans la foule portaient désormais des smartphones et autres appareils compatibles Internet dans leurs poches. Ils étaient prêts à fournir des mises à jour en direct, à prendre des photos et des vidéos à tout moment et à les partager instantanément sur les médias sociaux avec leurs supporters dans tout le pays et au-delà.* » (Gruzd, Tsyganova, 2014).

Dans le cadre de nos travaux nous avons choisi Twitter car c’était le seul média social qui a connu un développement spécifiquement lié aux évènements. Twitter fait partie des outils de micro-publication. Les services de micro-publication ou micro-blogs sont : « *une version*

miniature de blogs auxquelles s'ajoutent des capacités de réseau social et de mobilité » (Barnes et Böhringer op. cit.). Ce service, créé en 2006, est rapidement devenu un espace de création, diffusion, commentaire d'informations. Les utilisateurs disposent de 140 caractères (jusqu'en janvier 2016) pour : « *en plus de la communication interpersonnelle, Twitter est de plus en plus utilisé comme source d'information en temps réel, comme lieu de débat sur les actualités, la politiques, les affaires, les divertissements* » (Weller, 2013). Également appelé le sms d'internet, Twitter est devenu en l'espace de quelques années un outil incontournable pour le suivi d'événement, d'émotions, et en temps réel et différé.

En 2015, Twitter rassemblait 320 millions d'utilisateurs actifs chaque mois en faisant le huitième média numérique le plus utilisé dans le monde. Cependant, ce classement ne reflète pas l'utilisation spécifique que ses utilisateurs en font et comment Twitter se distinguent des autres médias sociaux ni les restrictions qu'il impose. En effet si les autres médias sociaux font la part belle à la grande liberté d'expression et la multiplicité des contenus médiatisés, Twitter impose une contrainte forte : 140 caractères pour exprimer l'intégralité de sa pensée.

Twitter a joué un rôle particulier avec un positionnement significatif dans la mesure où il était peu employé avant les grandes manifestations avant d'être utilisé massivement à travers toute la période (plus de 40 millions de tweets). En novembre 2014, soit une année après le début des évènements en Ukraine, Yandex, le plus populaire moteur de recherche de l'espace russophone, publiait une étude sur l'évolution de l'utilisation de Twitter dans le pays entre juillet 2013 et juillet 2014. Parmi les enseignements de cette étude plusieurs points viennent confirmer l'intérêt d'étudier les réseaux dans le contexte d'un conflit.

En novembre 2013 et novembre 2014, le nombre d'ouvertures de compte autant que l'activité de chaque compte ont augmenté de façon spectaculaire. Depuis juillet 2013 Twitter progressait à un rythme de 6 000 à 7 000 nouveaux comptes créés chaque mois. En décembre, ce nombre a atteint 16 000 ouvertures, et en janvier 2014, 55.000.

- Volumétrie par rapport aux évènements

  Twitter a connu deux pics d'ouverture de comptes : en janvier suite aux évènements de Maidan et en juillet à la suite du crash du MH117. Ce fait illustre la volonté des parties prenantes d'utiliser Twitter, ou plutôt un outil de diffusion et de suivi d'information public et instantané comme outil d'information/communication au moment d'événements significatifs.

- Ouverture de comptes par rapport à la géographie

  Entre juillet 2013 et juillet 2014, la plupart des nouveaux comptes, en volumétrie, se sont ouvert à Kiev (capitale, lieu des affrontements initiaux) et dans la ville de Dniepropetrovsk (située sur la frontière avec la région séparatiste du Donbass). En pourcentage de progression, les villes situées à l'ouest du pays, connues pour leur sentiment nationaliste, sont celles qui ont connues le plus fort taux de croissance d'ouverture de comptes dû au fait que très peu de compte étaient ouverts initialement. Au total, le nombre de comptes actifs est passé de 282 000 à 591 000 pour une population estimée à environ 42 millions de personnes. Fait caractéristique de l'ouverture de compte en Ukraine pendant cette période, 85% des utilisateurs déclarent leur position dans leur profil ce qui paraît particulièrement élevé.

- Volumétrie des émissions

  Entre juillet 2013 et janvier 2014, les twittos ukrainiens publiaient en moyenne 80 000 messages par jour. Suite à l'annexion de la Crimée par la Russie fin février 2014 le nombre de message passe à 180 000 par jour. L'activité a été soutenue de façon relativement similaire de février à juin avant le pic de juillet 2014. Rien que le 20 février 2014, lorsque des dizaines de manifestants ont perdu la vie dans le centre-ville de Kiev, 240 000 tweets ont été diffusés.

- Langue employée

  Parmi les enseignements issus de l'étude de Yandex et confirmés par notre plateforme, la première surprise vient de l'utilisation de la langue russe majoritairement par les twittos, ce que plateforme DETEVEN confirme cela avec un score de détection de la langue de 98% en faveur du russe.

- Utilisation des hashtags, importance du toponyme

  Le hashtag le plus populaire de cette période était Euromaidan dans toutes ses translittérations (russe, latine, anglo-saxonne, etc.). Cependant dans le top 20 des hashtags les plus utilisés sur la période, 10 d'entre eux utilisent un toponyme d'un pays ou d'une ville. (Yandex 2014b).

Dans notre jeu de données sur les 22 millions de tweets émis en russe ou ukrainien entre novembre 2013 et juin 2014, 13 millions de tweets entre novembre 2013 et juin 2014 contiennent un toponyme correspondant à un lieu en Ukraine. Avec 59% des tweets contenant

un ou plusieurs toponymes pendant une période aussi crisogène on peut donc estimer que des pics d'apparition de ces toponymes devraient correspondre à des moments de tensions dans le conflit sur les lieux mentionnés. Une étude comparant les tweets d'une crue à ceux d'un feu remarque la plus grande utilisation de toponyme dans le cadre du feu car les émetteurs subissent en temps réel l'impact immédiat de l'évènement alors que dans une crue la montée des eaux peut être plus progressive générant du contenu majoritairement sans mention de toponyme (Vieweg et al., 2010). L'utilisation de toponymes augmente significativement avec la survenue d'un événement majeur et il parait logique que les personnes s'exprimant sur un évènement à impact immédiat, tel qu'un conflit armé mentionnent le lieu de l'évènement.

La détection d'entités nommées plus particulièrement de toponymes se base sur des données référencées dans un index géographique ou gazetteer. Il n'existe pas d'index complet et le choix de l'index fait significativement varier les résultats (Jurgens et al., 2015). Pour compenser cela nous avons fait une détection sur les 459 villes reconnues par le parlement ukrainien (rada.gov.ua, 2018). Même si comme cela a été démontré, la mention d'un lieu dans un message limité à 140 caractères reste limitée et la prise en compte des versions vernaculaires ou tronquées complique la détection, la mention géographique n'implique pas directement la présence de l'émetteur sur le lieu en question (Han et al., 2014). Pourtant ces limitations démontrées sur des volumes de données variées et à travers le temps semble disparaître en période de crise. Cette détection de pic de mention, où un pic est défini comme un mot qui apparaît soudainement fréquemment dans une fenêtre temporelle et dont l'occurrence dure plus d'une minute, est remarquable dans notre jeu de données.

Sur la période du 1er avril 2014 au 31 mai 2014 nous suivons plus particulièrement les mentions des toponymes de villes situées dans l'Est de l'Ukraine, au cœur de la zone de conflit : Slaviansk (Славянск) ; Kramatorsk (Краматорск) ; Marioupol (Мариуполь) ; Berdiansk (Бердянск) ; Volnovakha (Волноваха) ; Artemosk (Артёмовск) ; Rubejnoe (рубежное) ; Gorlivka (Горловка) ; Lougansk (Луганск) ; Donetsk (Донецк). Ces toponymes sont détectés quelle que soit leur déclinaison.

On observe deux catégories de ville, celles qui par la faible population ou par le faible taux de pénétration de twitter n'était que faiblement mentionnée avant que la crise ne les impacte (moins de 500 mentions/jours) et celle qui avait un nombre de mention volumineux avant la crise. Dans les villes à faible volumétrie initiale il y Berdiansk, Volnovakha, Gorlovka,

Kramatorsk, Slaviansk., Artemosk (Артёмовск) ; Rubejnoe (рубежное) Dans les villes à forte volumétrie initiale il y a Donetsk, Lugansk et Marioupol.

La courbe de mention de la ville de Volnovakha est caractéristique dans la mesure où elle est mentionnée dans 7 tweets en moyenne par jour puis atteint un pic à plus de 4500 le 22 mai suite à une attaque d'un check-point de l'armée par des séparatistes.

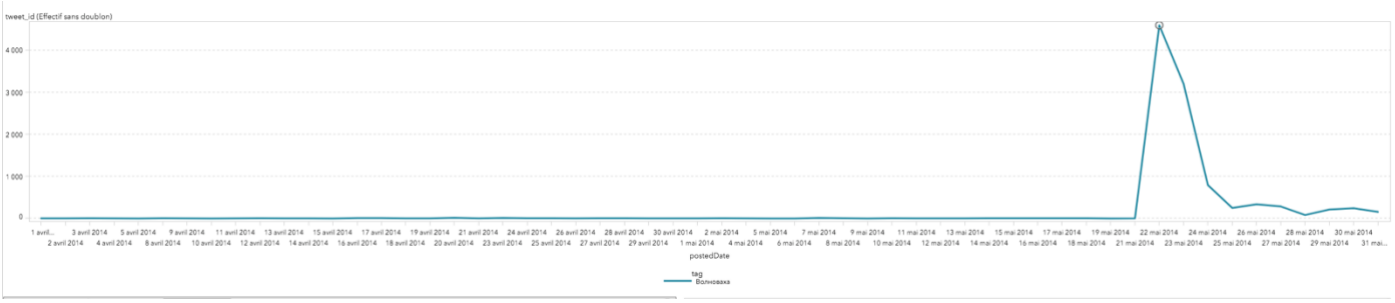


Figure 18, graphique 2 : Détection d'activité de la Ville de Volnovakha, janvier à juin 2014, extrait de la plateforme DETEVEN

Autre courbe caractéristique, celle de la ville de Gorlovka où chaque pic de mention correspond à un moment de tension voire d'affrontement entre les forces en présence.

Figure 19, graphique 3 : Détection d'activité de la Ville de Gorlovka, janvier à juin 2014. Extrait de la plateforme DETEVEN

La ville de Slaviansk connait, elle, un début d'activité le 12 avril passant d'une valeur médiane de 24 mentions du 1er au 12 avril à plus de 4 000. Le 12 avril date de sa prise par les

séparatistes. Devenue une place forte des séparatistes, La ville gardera une forte activité même si des pics apparaissent à chaque évènement significatif.

Figure 20, graphique 4 : Détection d'activité de la Ville de Slaviansk, janvier à juin 2014. Extrait de la plateforme DETEVEN

Pour les villes à forte volumétrie initiale, on observe la même tendance à générer des pics de mentions lors des évènements crisogène. La ville de Donetsk était mentionnée plusieurs centaines de fois avant le conflit et maintient un niveau élevé durant le conflit. Pourtant, des pics remarquables restent observables. Ils correspondent chacun à une situation de crise aggravée.

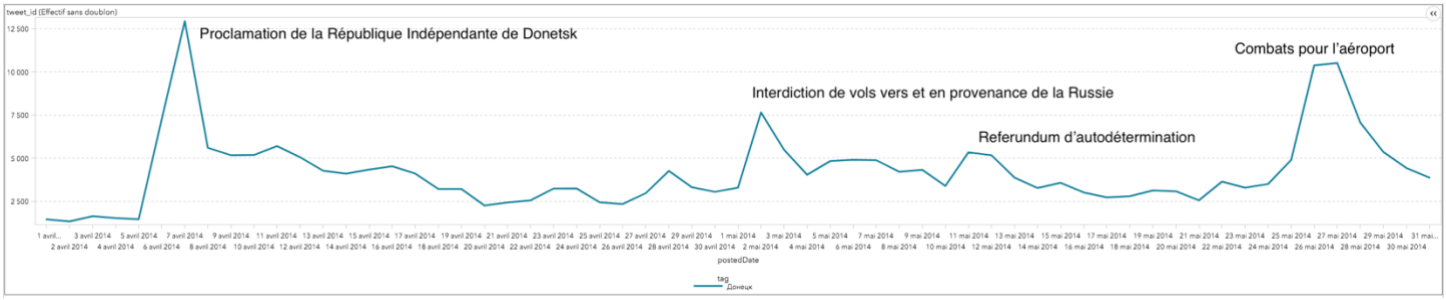


Figure 21, graphique 5 : Détection d'activité de la Ville de Donetsk, janvier à juin 2014. Extrait de la plateforme DETEVEN

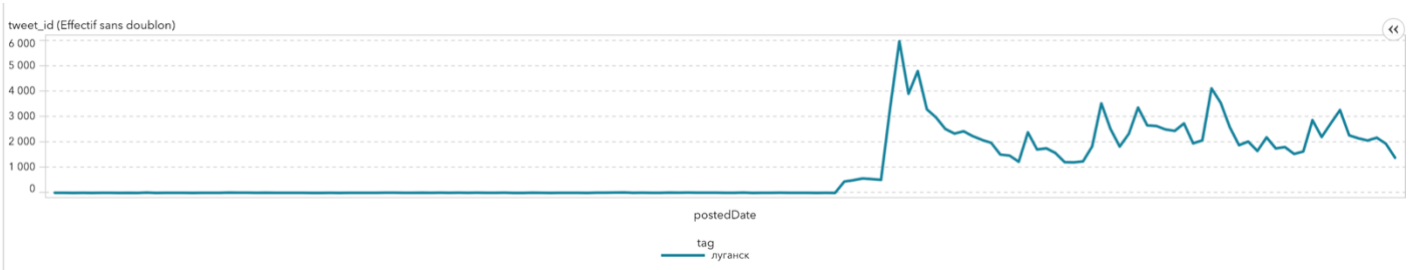


Figure 22, graphique 6 : Détection d'activité de la Ville de Lougansk, janvier à juin 2014. Extrait de la plateforme DETEVEN

La ville de Lougansk n'est quasiment jamais mentionnée entre le 1er janvier et le 5 avril malgré les évènements sombres qui secouent le pays. Cependant dès le mois d'avril sont nombre de

mention explosent et chaque étape de la guerre séparatiste marquera le pouls de la ville au travers des tweets la mentionnant.

Les éléments observés issus du conflit ukrainien montrent qu'en période de crise l'augmentation du nombre de mention d'un toponyme est un indicateur d'événement. Ce constat se vérifie tant en forte qu'en faible volumétrie. Reste à savoir qui est à l'origine de l'information, notamment s'il s'agit de sources locales ou relayées. Certaines catastrophes naturelles de par leur fréquence sont constamment suivies par des agences disposant d'équipements de surveillance plus sensibles que la perception des humains, il paraît plus probable dans ces contextes que l'information soit diffusée par un organisme spécialisé puis relayée par Twitter. Dans ces cas, les utilisateurs de Twitter ne génèrent du contenu que post-évènement pour exprimer des ressentis ou des impacts. Pour ce qui est des crises sociales, il n'exsite pas d'appareil connecté susceptible de les détecter, même si la question reste posée quant aux premiers émetteurs. Qui des médias où des utilisateurs sont le plus susceptible de diffuser l'information en premier ?

Si l'on considère l'incident du 22 mai à Volnovakha, le graphique 7 ci-dessous indique que parmi les principaux émetteurs relayant l'évènement se trouvent des médias officiels et officieux (représentant les parties belligérantes).

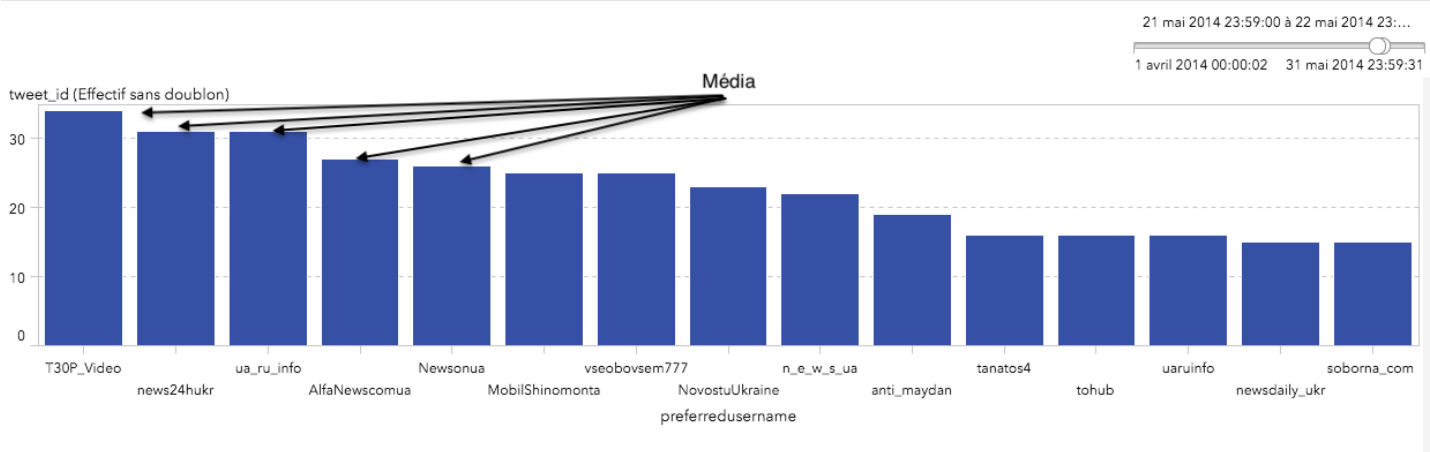


Figure 23, graphique 7 : Identification des sources des tweets mentionnant l'attaque de Volnovakha le 22 mai 2014. Extrait de la plateforme DETEVEN

Lorsqu'on regarde la diffusion chronologique des tweets on observe que les primo-émetteurs relaient des éléments d'information d'un média séparatiste diffusant sur l'application Zello. Le reste des tweets relatant le contenu sont des liens vers des médias. L'ensemble des contenus est formaté comme des titres de presse.

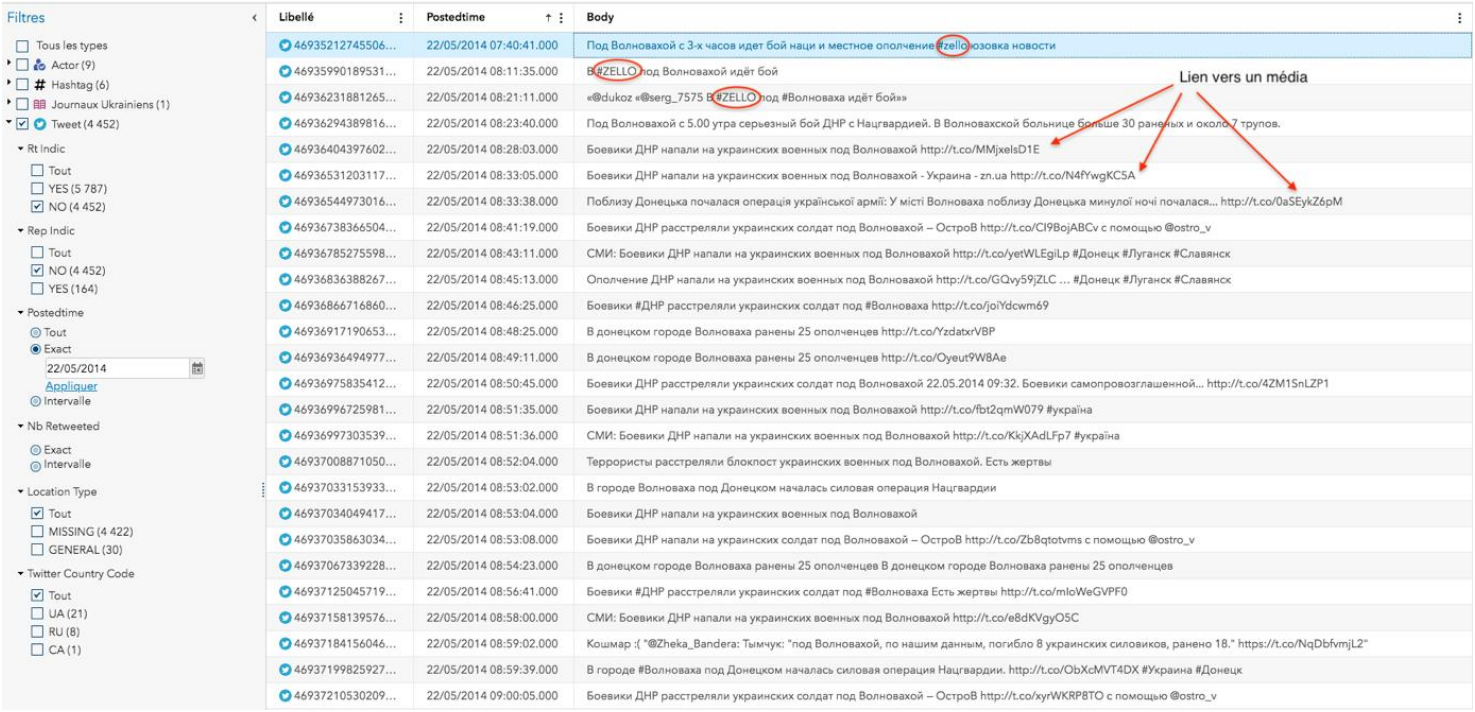


Figure 24, tableau 4 : Mention du média séparatiste Zello dans les tweets mentionnant l'attaque de Volnovakha. Extrait de la plateforme DETEVEN

Cela peut s'expliquer parce que l'attaque a eu lieu en périphérie de la ville, où la probabilité de témoins disposant d'un compte twitter est plus faible, et par le fait que les séparatistes ont privilégié la diffusion de l'information par un média sous leur contrôle plutôt qu'au moyen d'une plateforme occidentale. Par contre, si l'on considère l'attaque sur Slaviansk le 2 mai, on remarque très clairement la plus grande présence d'individus par rapport aux médias qui ne représentent que deux sources sur les quinze plus grandes en volumétrie.

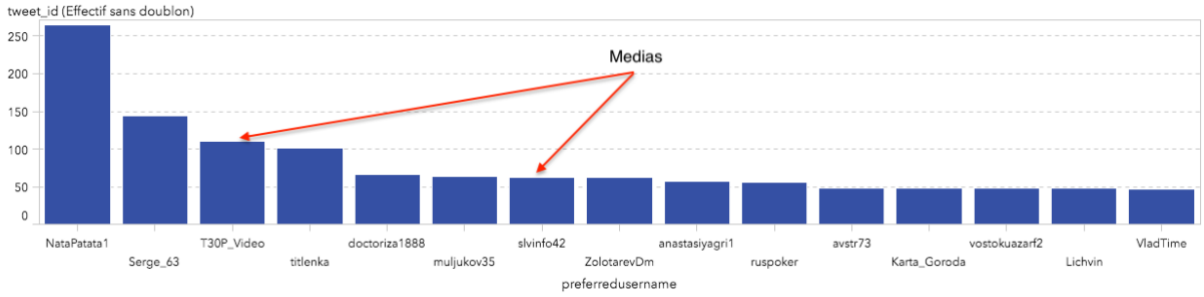


Figure 25, graphique 8 : Primo-émetteurs twettant sur l'attaque de Slaviansk le 2 mai 2014. Extrait de la plateforme DETEVEN.

De plus, parmi les premiers tweets on observe les annonces de l'attaque (1), puis des tweets plus locaux tels que le fait que les journalistes étrangers quittent la ville (2), la mention du fait qu'on entend les tirs, les blindés, les hélicoptères (3) et la précision accrue de la géolocalisation des affrontements par indication d'un site spécifique (4), autant de signaux indiquant la proximité géographique de l'émetteur avec l'évènement c'est à dire d'individus localisés dans la ville.

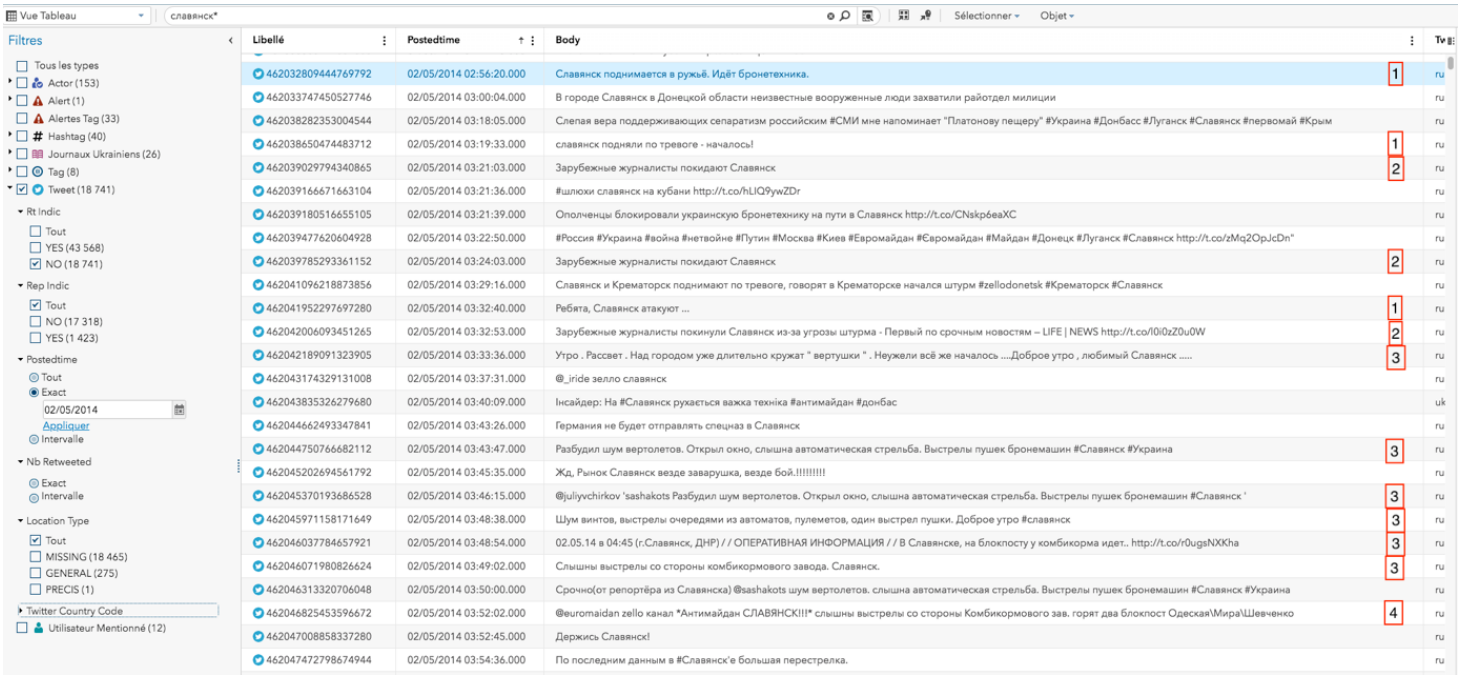


Figure 25, tableau 5 : Premiers tweets émis lors de la première offensive sur Slaviansk par les forces armées ukrainiennes le 2 mai 2014. Extrait de la plateforme DETEVEN

Traduction :

1/ 02 :56 :20 : les canons réveillent Slaviansk. Les blindés arrivent

2/ 03 :21 :03 : Les journalistes étrangers quittent Slaviansk

3/ 03 :24 :03 : Matin. Aube. Les hélicoptères tournent depuis longtemps au-dessus de la ville. Cela a-t'il vraiment commencé ? Bonjour Slaviansk mon amour

Une fois le sous-évènement détecté par mention de toponyme, l'analyse sémantique permet de déterminer s'il s'agit d'une reprise d'un média distant ou d'un témoin direct. La présence de mots liés aux sens (vue, ouïe, odorat, goût, touché) est un fort indicateur de proximité du témoin.

5.5. Conclusion

Ce déferlement d'évènements en Ukraine, est une illustration parfaite du concept du continuum sécurité-défense où des incidents de sûreté publique dégénèrent en opportunité pour une révolution c'est-à-dire où l'affaiblissement des structures d'État entraine le chaos d'une guerre civile. Les médias sociaux sont employés par toutes les parties prenantes à un conflit et leur utilisation dans ces moments porte des caractéristiques qui permettent de distinguer les « évènements » des occurrences normales du quotidien dont notamment une forte augmentation d'ouverture de compte et une utilisation des toponymes dans les contenus supérieurs à la moyenne.

Nous avons décrit la possibilité de détecter des événements par pic de mention de toponymes en observant les sous-évènements du conflit ukrainien. Cette méthode fonctionne tant sur des petits volumes que sur des grands volumes de tweet. De plus nous avons montré que la proximité géographique n'influait pas négativement sur la détection de l'évènement, mais plutôt sur la nature de la source. Dans le premier cas, l'évènement est annoncé principalement par des médias externes et dans le deuxième par des individus sur zone.

Cette méthodologie simple, peu coûteuse en ressources et largement automatisable, et qui peut être supervisée par une intelligence artificielle (pour ajuster le seuil de détection), permet une supervision de larges territoires en conflit, à distance, comme celle réalisée par des organismes internationaux de prévention de conflit tels que l'OSCE et l'ONU ou des services de renseignement. Elle permet également de réunir efficacement un large corpus de tweet pour procéder à une protest event analysis manuelle ou assistée. Enfin nous proposons de pousser plus loin la mise au point d'algorithmes permettant la détection d'évènements crisogènes permettant le filtre des tweets, l'association d'un poids à chacun en fonction de son potentiel degré de pertinence du tweet quant au fait que l'émetteur soit une source primaire ou non, la prise en compte des relations entre les individus au-delà du contenu textuel. L'algorithme aura aussi pour objectif de permettre un suivi temporel de l'évolution de ces topics par le biais de différentes méthodes d'agrégation de ces topics sur des intervalles de temps consécutifs.

6. Chapitre 6 : l'exploitation analytique des données.

6.1. Introduction

Les réseaux sociaux nous ont semblé intéressants comme source de données pour les PEA parce qu'ils correspondent en grande partie aux critères de Koopmans pour la sélection de sources : continuité (ils diffusent de manière continuent pendant tout le conflit), fréquence (la diffusion doit être régulière), qualité (ils sont reconnus en tant que source d'informations de haute qualité au vu du nombre d'études portant sur leurs données), portée nationale: ils couvrent l'ensemble du territoire malgré des sources émettant depuis le principales villes, couleur politique (toutes la panoplie des opinions possibles est exprimées sur les réseaux sociaux). La sélectivité est le seul point que nous ne prenons pas en compte dans la mesure où nous n'étudions qu'un seul réseau social dont les biais ont été exprimés précédemment (Koopmans, et Rucht 2002). Plusieurs approches sont possibles pour exploiter des données de masses, notamment des analyses statistiques, sémantiques, relationnelles qu'elles soient appliquées à des jeux de données qualitatifs ou quantitatifs. Comme décrit dans le chapitre précédent, un tweet est composé de données non structurées (body, hashtag) et structurées (tout le reste). La difficulté liée à l'exploitation des données non structurées vient essentiellement des processus d'exploitation. Dans ce chapitre nous allons comparer une journée de manifestation ordinaire, le 5 janvier 2014, à des affrontements violents les 19 janvier et 20 février. Les outils mis en place nous permettront de dégager des règles de détections d'évènements significatifs dans un conflit. Pour tester la validité de ces règles, nous les appliqueront à un autre moment du conflit le début de la guerre civile : le mois d'avril 2014. L'objet de ce chapitre est de caractériser les indicateurs d'une journée de crise. Nous étudierons les volumes d'émissions de tweets et retweets, les sujets abordés, les sources d'émission au travers d'outils d'analyse statistique, sémantique et relationnelle. Il est question ici, d'être en mesure de construire les composants d'un modèle de données, c'est-à-dire d'identifier rapidement les variables d'intérêt pour l'analyse, de réduire la dimensionnalité de jeux de données très fournis, et de créer aisément de nouvelles variables à partir du jeu de donnée original. Pour ce faire, nous explorerons à l'aide d'une interface visuelle pour contribuer à la détection des tendances, des corrélations ou des modèles/schémas (pattern) dans les données.

6.2. L’analyse statistique visuelle des données

Les outils d’analyse visuelle, basés sur la statistique sont particulièrement utiles pour le Protest Event Analysis. Lorsqu’ils sont appliqués à des données issues des réseaux sociaux il est nécessaire de bien comprendre ces données notamment leur taille c’est-à-dire le nombre d’observations prises en compte et leur cardinalité nombre de valeurs uniques dans la colonne. Ainsi une colonne indiquant si un tweet est un retweet aura deux options oui ou non donc une cardinalité faible alors qu’une colonne indiquant le contenu d’un tweet aura une cardinalité quasi infinie. Dans le cas de Twitter, les premiers éléments à prendre en compte sont la volumétrie des tweets et des retweets, et les émetteurs de ces derniers. Il faut donc choisir un rendu visuel cohérent avec les données que l’on souhaite explorer.

L’analyse visuelle statistique permet de rapidement attirer l’attention d’un analyste sur les évènements clefs pour une observation ou une détection d'anomalies. Cela permet également de pré-visualiser les données sans être influencé par leur contenu et ainsi se laisser surprendre par les données avant de les explorer pour détecter les tendances, les corrélations afin de créer une règle de base pour une stratégie de suivi d’évènement dans le futur. Il est important d’avoir un lien direct avec la donnée brute depuis le tableau de bord afin de pouvoir toujours vérifier si l’anomalie ou la corrélation est bien quelque chose de significatif et pas une erreur de codage. Le système que nous utilisons s’exécute sur un serveur d’analyses en mémoire très évolutif appelé serveur LASR de SAS. Il permet aux utilisateurs de visualiser et d’analyser d’énormes quantités de données en quelques secondes. Il permet notamment aux utilisateurs de créer des calculs de données avancés en direct, sans qu'il soit nécessaire de modifier la préparation des données en amont. Ils peuvent contenir une logique booléenne, des calculs temporels et des opérateurs de texte. Ces calculs sont alors immédiatement disponibles pour analyse. La découverte visuelle des données incite l’analyste à se concentrer sur les évènements remarquables, leurs caractéristiques et leurs relations. Enfin la plateforme permet d’utiliser de nombreux filtres tels que des filtres temporels et la corrélation automatisée par exemple pour voir qui a tweeté le premier ou qui a été le plus retweeté à un instant précis du conflit afin d’identifier des témoins directs ou des influenceurs parmi les émetteurs. L’avantage d’une visualisation interactive est la capacité à tester des hypothèses en temps réel.

Dans le premier tableau de bord que nous avons mis en œuvre nous étudions les éléments suivant (dans le sens des aiguilles d’une montre) : suivi des émissions de tweets uniques, suivis

des émissions de retweets, suivi des comptes les plus actifs, suivi des comptes les plus retweetés. Nous utilisons trois sortes de représentations graphiques : le graphique linéaire, le diagramme à barres, et un graphique en mosaïque.

Figure 26 : Suivi des tweets et de leur émetteur

Les graphiques linéaires montrent la relation d'une variable à une autre. Ils sont le plus souvent utilisés pour suivre les changements ou les tendances au fil du temps lorsque l'analyste cherche à identifier des tendances, des pics ou des creux remarquables. Les graphiques linéaires sont également utiles pour comparer plusieurs éléments sur une même période. C'est que nous illustrerons sur la partie intégration des outils sémantiques. Dans le graphique linéaire de la figure 26 nous avons en ordonnées le volume émis et en abscisse la date d'émission. Sur la période du 1er au 31 janvier 2014 nous avons collecté 1 180 357 tweets dont 363 746 retweets soit environ 31%.

L'analyse qui peut être faite sur la volumétrie en étude rétrospective doit prendre en compte avec attention le créneau de temps observé. Il est ici question de choisir le bon point de vue : stratégique, opérationnel et tactique. En effet si l'on étudie un évènement de façon trop isolée, les pics et les creux peuvent apparaître très remarquables alors qu'ils ne le sont pas forcément lorsqu'ils sont observés sur une série temporelle plus longue. Au contraire, une observation sur un créneau de temps trop long à tendance à lisser les courbes et à faire disparaître les sous-évènements et signaux faibles.

Ci-après la période correspondant au mois de janvier 2014 à trois échelles, figure 27, 28, 29 :

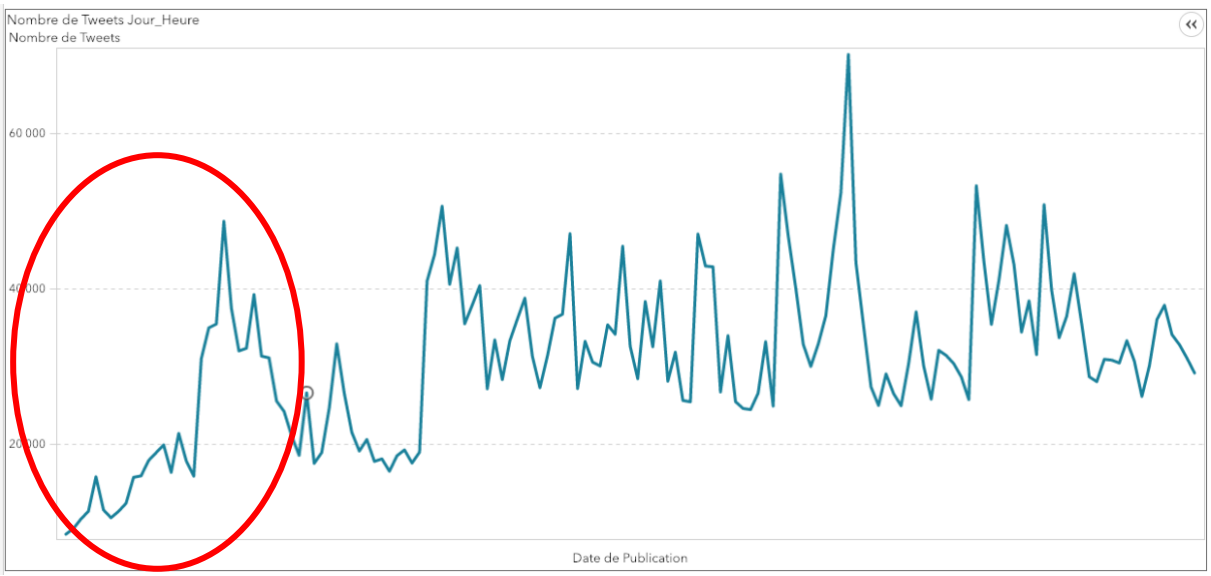


Figure 27 : Volumétrie des tweets sur une échelle de 5 mois

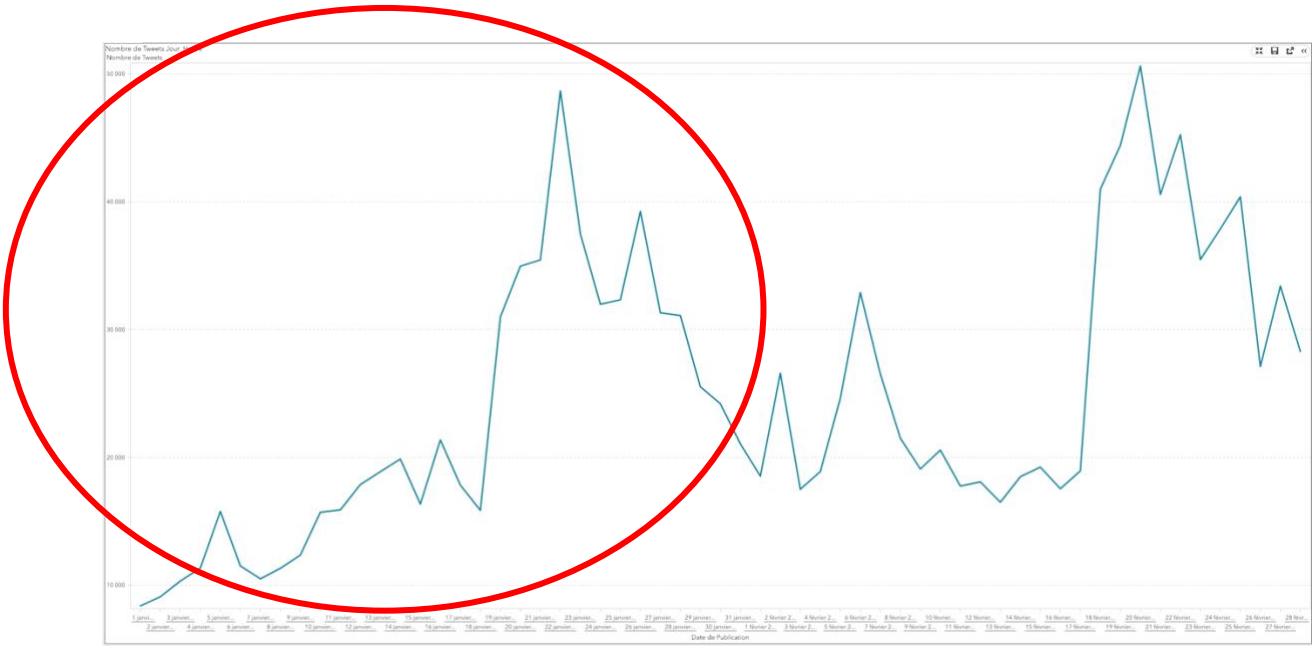


Figure 28 : Volumétrie des tweets sur une échelle de 2 mois

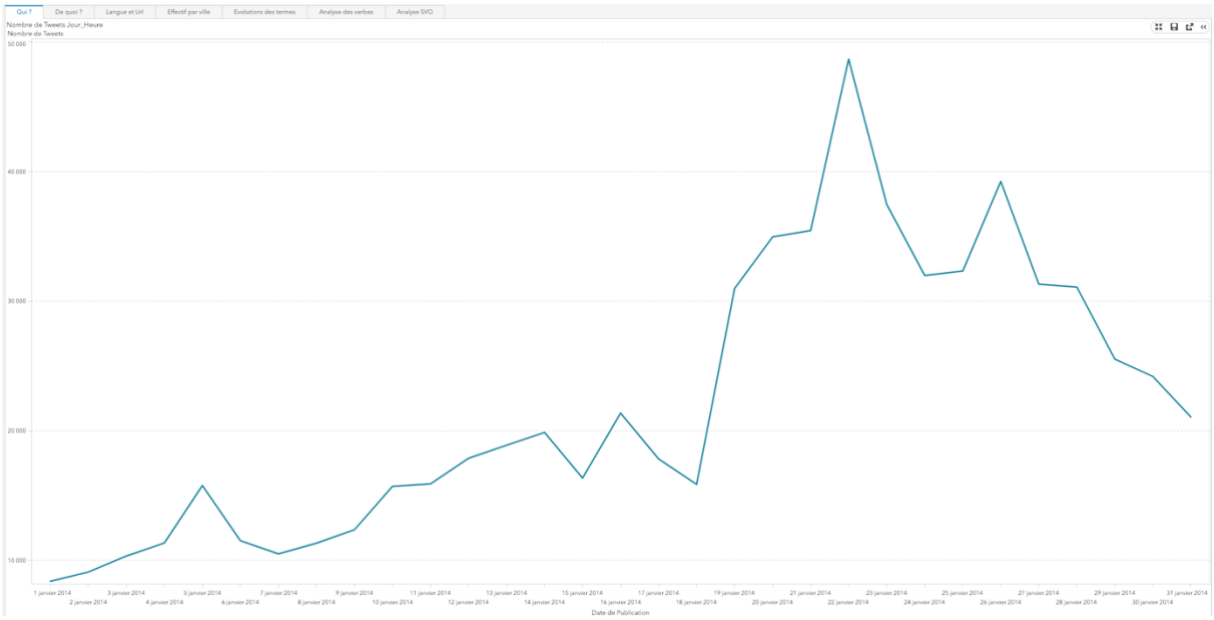


Figure 29 : Volumétrie des tweets sur une échelle d'un mois

Au vu des différentes échelles, l'échelle sur deux mois permet de distinguer les évènements et leurs sous-évènements de façon plus nette que les deux autres échelles.

Analyse du mois de janvier au travers du graphique linéaire, figure 29 :

Le pic du 5 janvier correspond au rassemblement populaire, le « Veche » du dimanche en place depuis le mois de décembre 2013. Voir figure 30.

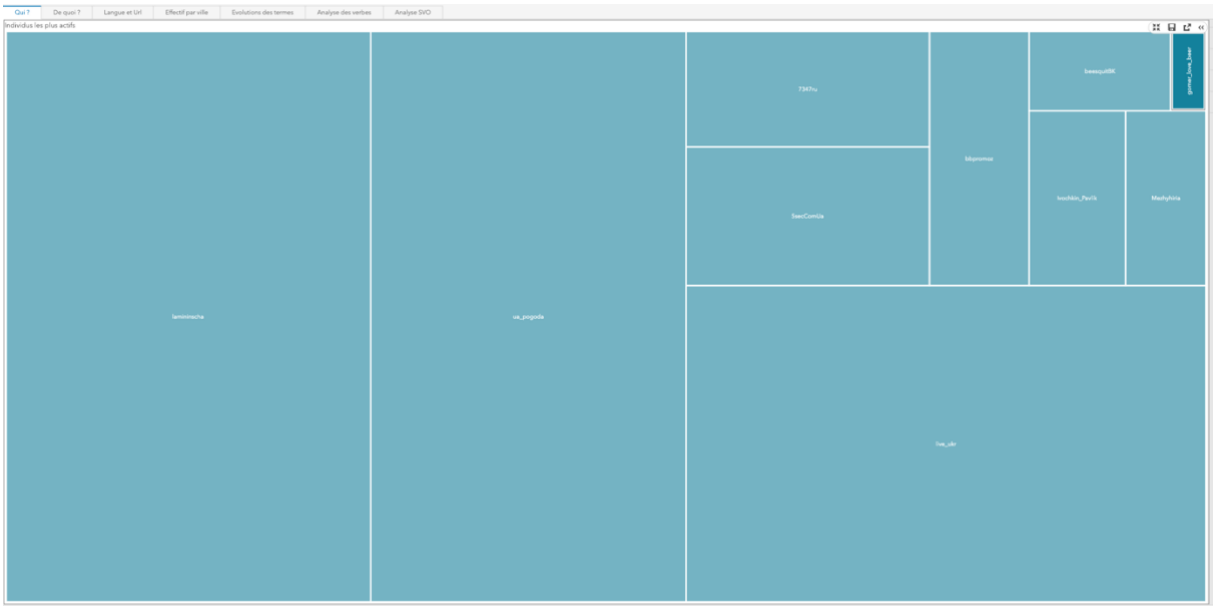


Figure 30 : Mosaïque des émetteurs les plus prolifiques

Le graphique en mosaïque, figure 30, nous indique que les 5 plus gros des émetteurs ce jour-là malgré l'évènement sont dans l'ordre de volume d'émission décroissant :

- compte à vocation commerciale lamininscha, créé en septembre 2013
- compte de prévision météo ua_pogoada, créé en octobre 2012
- compte d'information live_ukr, créé en décembre 2013
- compte à vocation commerciale 5secComUa, créé en mai 2013
- compte à vocation commerciale 7347.ru, créé en 2011

Seul le compte live_ukr sort du lot car il s'agit non seulement d'un site d'information, mais il a, en plus, été créé au moment du conflit. Il mérite donc d'être suivi pour voir s'il fournit des informations pertinentes par rapport aux évènements que nous souhaitons observer.

Si l'on observe maintenant le graphique des retweets de la journée du 5 janvier 2014, figure 31 :

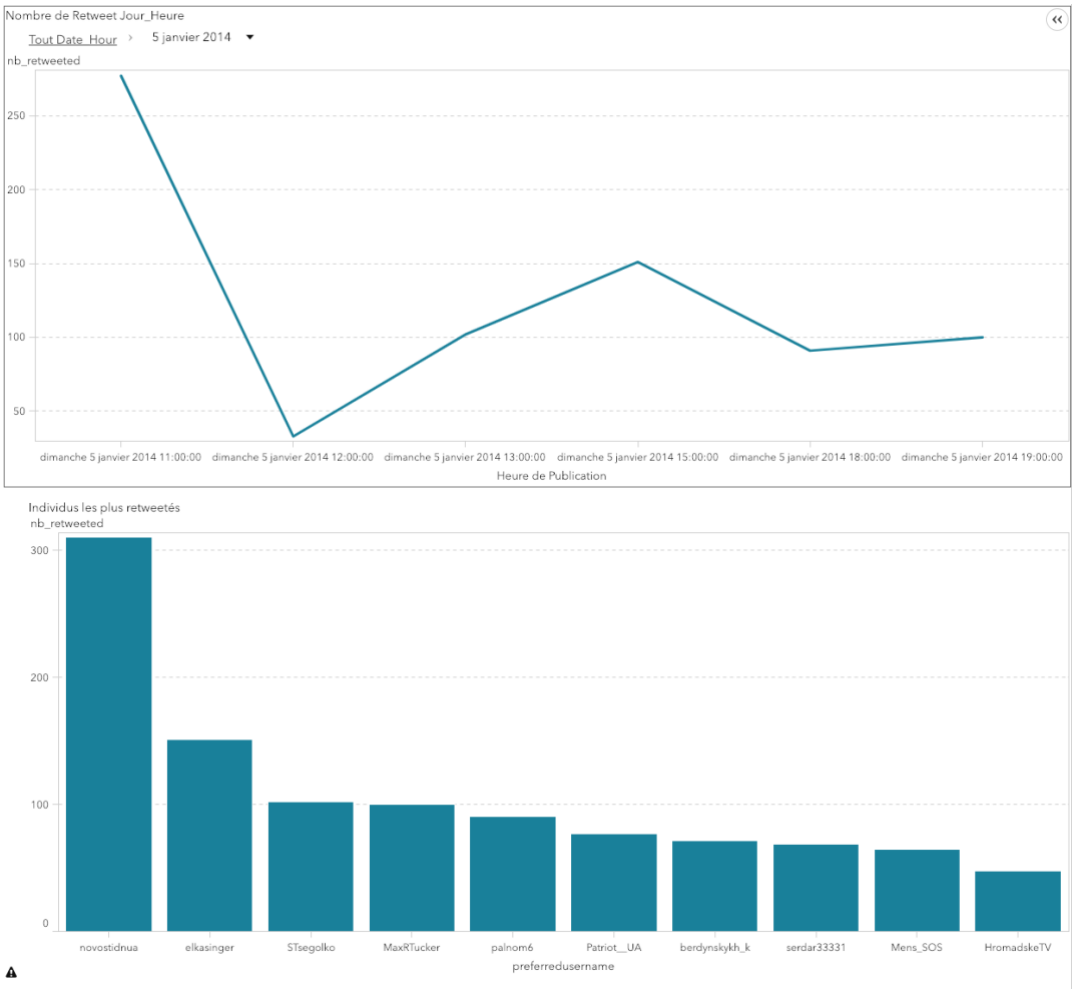


Figure 31 : Graphique des retweets du 5 janvier 2014

Le pic maximum de retweet a eu lieu à 15h et les comptes les plus retweetés à ce moment-là étaient :

- tweet d'une chanteuse : elkasinger
- tweet d'une journaliste : berdynskykh_k
- tweet d'un homme politique o_tiahnybok
- tweet d'une station radio financée par le congrès américain : radiosvoboda
- tweet d'un journal ukrainien : onlinekpru

Les graphiques à barres sont le plus souvent utilisés pour comparer les quantités de différentes catégories ou groupes. Les valeurs d'une catégorie sont représentées à l'aide des barres et peuvent être configurées avec des barres verticales ou horizontales, la longueur ou la hauteur de chaque barre représentant la valeur.

Lorsque le tableau de bord paraît pertinent par rapport à la nature et au volume des données on peut s'en servir dynamiquement pour explorer les différentes séquences détectées sur la période choisie.

La période de deux mois janvier/février 2014 (figure 28) correspond à un moment significatif dans le conflit ukrainien car elle regroupe deux phases : celle du durcissement de la répression et celle de la chute du gouvernement. Le graphique isole deux pics : un le 21 janvier qui est l'apogée d'une hausse initiée le 19 janvier et un second le 20 février qui est l'apogée d'une hausse initiée le 17 février.

Si l'on zoome sur le 19 janvier (figure 32), on observe les faits suivants :

Le graphique linéaire indique un point culminant à 16h avec un peu plus de 2500 tweet émis.

Le graphique mosaïque révèle que les acteurs les plus prolifiques étaient en termes de tweet uniques hors retweets :

- live_ukr : site d'information créé par les manifestants, 27 tweets
- radiosvoboda : station radio financée par le congrès américain, 21 tweets
- gurzuff : citoyenne ukrainienne, inscrite en octobre 2008, 8 tweets
- l_aquitaine : citoyen ukrainien (a priori) , inscrit en novembre 2012, 7 tweets
- vovakasko : citoyen russe (a priori), inscrit en décembre 2011, 7 tweets

Si l'on compare les émetteurs du 5 janvier à ceux du 19 janvier alors que le même type de rassemblement populaire a lieu, le volume de diffusion ne retombe pas dans le second cas. De plus on remarque l'absence de médias traditionnels, mais surtout la disparition des comptes à vocation commerciale remplacés par la participation de citoyens. Voir figure 32.

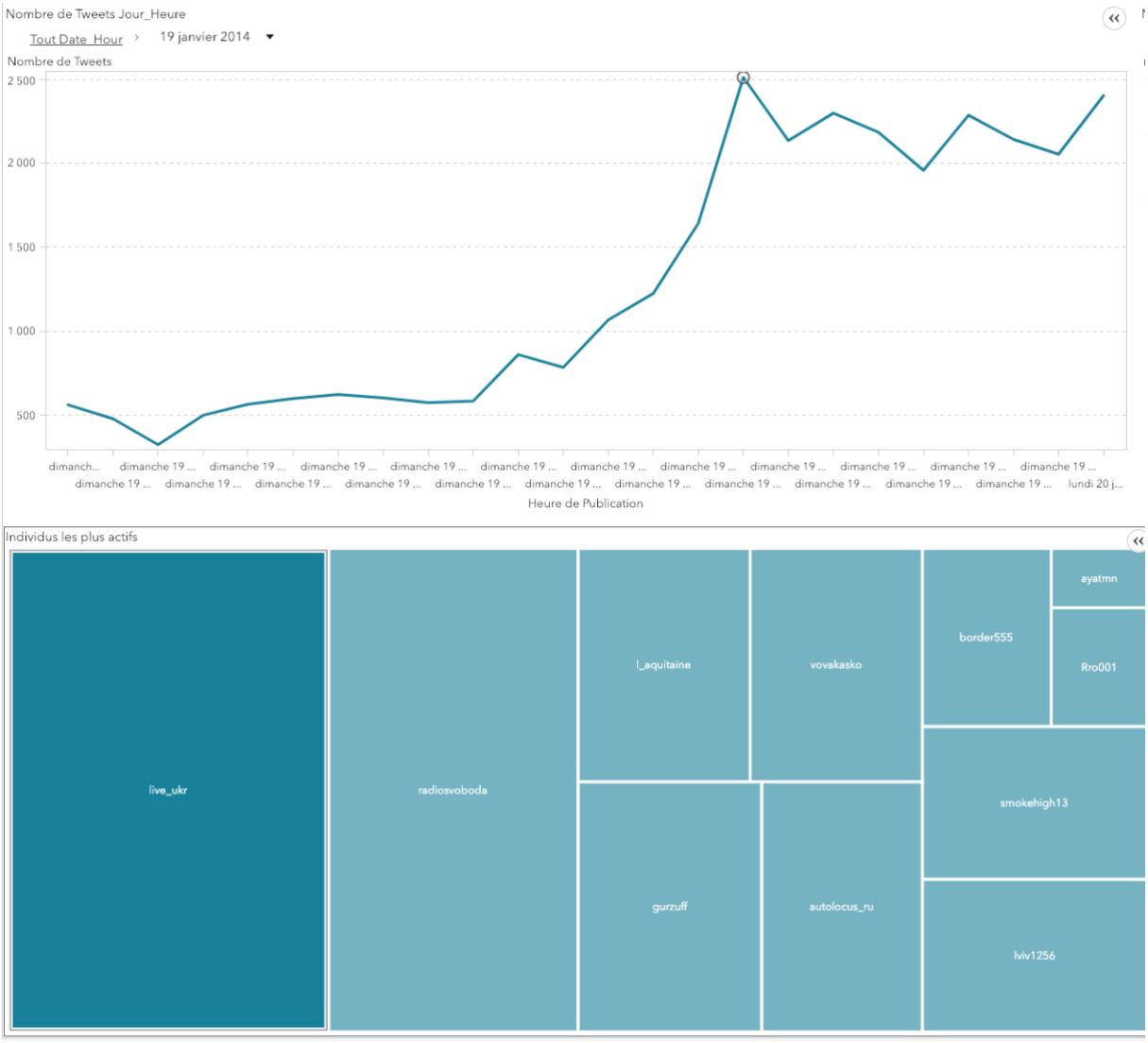


Figure 32 : Journée du 19 janvier

L'observation des graphiques du 19 janvier (figure 33) révèle également des différences significatives avec celui du 5 janvier : on trouve trois pics de retweet à 16h, 18h, 21h

A 16h : les sources les plus volumineuses sont en majorité des médias

- Avramchuk_katya : citoyenne postant un lien vers une page Facebook montrant les affrontements sur la rue Grushevskogo

- Sosmaydan : un des comptes des manifestants émet un tweet d'appel au secours pour demander la venue de médecins
- Tvrain, chaîne d'information d'opposition russe
- radiosvoboda
- tdanylenko, journaliste ukrainienne

A 18h : les sources les plus volumineuses sont en majorité des médias

- euroukraine
- radiosvoboda
- lifenews_ru, chaine d'information pro-russe
- euromaidan, un des comptes des manifestants
- PeterShuklinov, journaliste ukrainien

A 21h :

- euromaidan, un des comptes des manifestants
- ukpravda_news, compte d'un journal ukrainien
- grishynUA, journaliste pour un journal ukrainien, compte suspendu
- kulybysh, compte pro Ukraine, compte supprimé
- sosmaydan

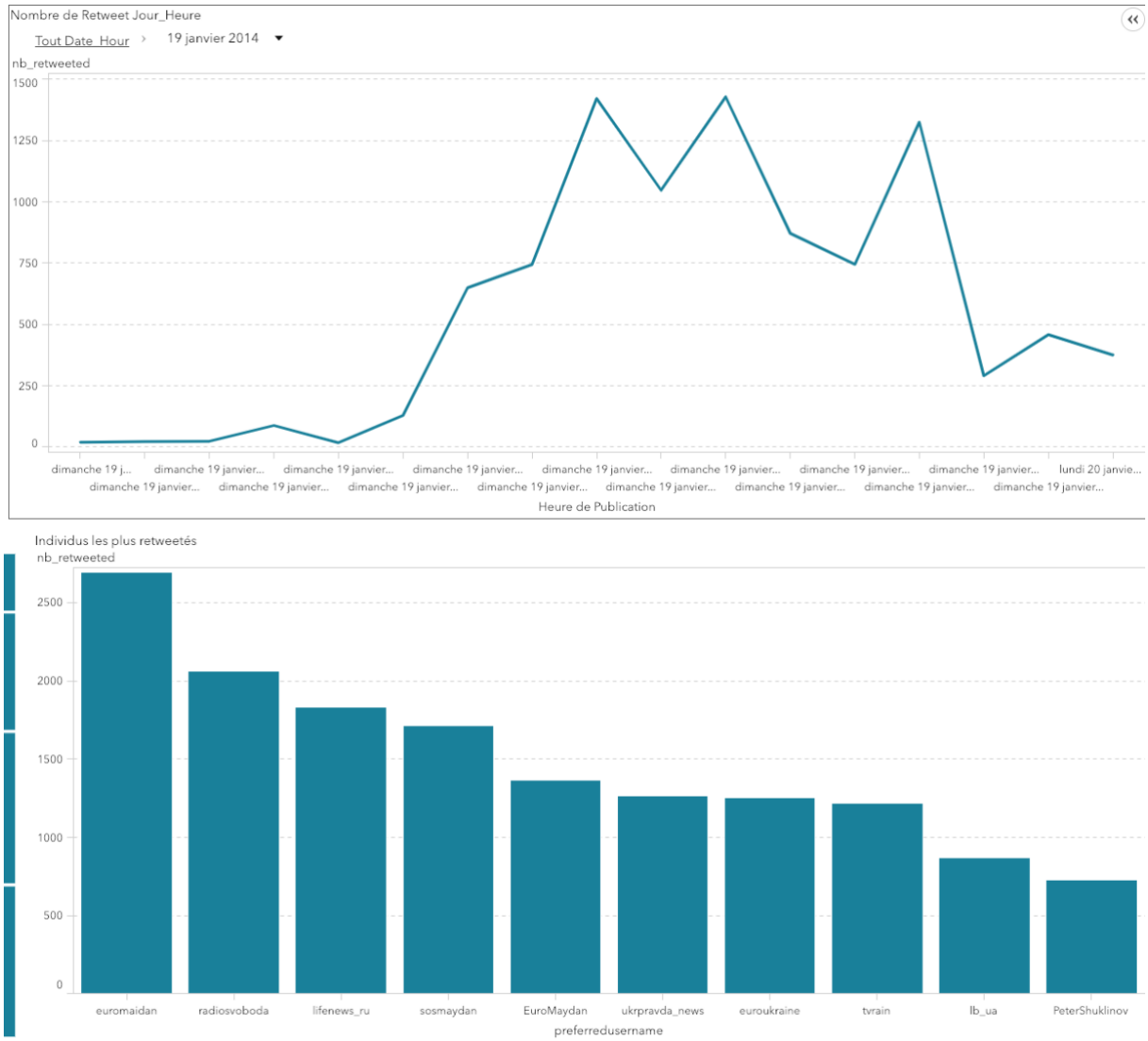


Figure 33 : Journée du dimanche 19 janvier

Lorsqu'on observe la journée du 20 février on constate de nouveau de multiples pics de retweets et une prédominance des médias et sites pro-manifestants.

Figure 34 : Journée du 20 février

Premières conclusions :

L'analyse statistique visuelle permet d'identifier les points éclairs d'un mouvement social au travers de la découverte interactive des données pour identifier facilement des tendances, des valeurs hors norme, etc. La représentation graphique automatique permet de sélectionner le graphique le mieux adapté pour afficher les données sélectionnées (graphique linéaire, histogramme, mosaïque, etc.). Un opérateur permettant de sélectionner précisément l'échelle de temps de plusieurs mois à quelques heures est indispensable pour pouvoir se positionner au juste niveau dans les données.

La principale contrainte de l'analyse statistique est qu'il faut connaître le réseau et la nature de données pour pouvoir créer des tables correspondant aux besoins de l'analyste. Elle requiert une conversation entre l'analyste et le data scientist pour exploiter au mieux les capacités de visualisation des données.

L'analyse statistique ne permet pas de comprendre la nature de l'évènement et il s'agit d'une forme d'analyse qu'il est particulièrement facile de tromper. En effet un réseau de bots (comptes automatisés) peut très facilement donner l'impression qu'une masse d'utilisateurs communique sur un sujet ou depuis un lieu donné.

Il est donc nécessaire d'utiliser une autre catégorie d'outils en combinaison pour mieux comprendre les données : l'analyse sémantique.

6.3. L’analyse sémantique visuelle

La recherche d’information contenue dans les tweets peut se faire de plusieurs façons. Lorsque des éléments clés de vos données tels que des noms, des dates, des mesures ou des relations de cause à effet sont dans un champ de texte libre, ils sont moins accessibles aux traitements par filtrage, et aux fonctions de recherche. L’outil employé doit permettre de récupérer les entités nommées extraites des tweets. Pour la reconnaissance d’entités nommées le système peut s’appuyer sur des concepts prédéfinis. Ils permettent d’extraire directement des informations sans un long travail de définition de concepts propres. Nous avons choisi dans un premier temps d’utiliser des dictionnaires pour augmenter la précision et la pertinence de l’apprentissage. L’effet est instantané sur l’ensemble des données accessibles à l’outil, le dictionnaire est appliqué à toute la base de données et fait ainsi ressortir les documents correspondants avec son nombre d’occurrences. Il est possible d’utiliser l’étiquetage morphosyntaxique afin d’extraire des informations en fonction du contexte de la phrase (adjectif, adverbe, verbe, …).

Soit on laisse la machine afficher les occurrences les plus fréquentes ou les plus anormales, soit on cherche de l’information que l’on pense devoir trouver. Cette dernière méthode est classiquement utilisée en PEA. En effet les éléments contenant l’information recherchée sont typiquement des articles de presse filtrés pour ne retenir que ceux qui contiennent une information portant sur le mouvement social, plus particulièrement ayant trait au répertoire d’action collective dudit mouvement. Cette sélection se fait au moyen d’un codebook dont le but est de maintenir une cohérence d’ensemble aux données.

Nous avons utilisé plusieurs indicateurs dans notre livre de codes pour filtrer les tweets recueillis pendant les manifestations. Ces indicateurs sont regroupés en concepts. Les règles de concept reconnaissent les éléments en contexte afin d’extraire uniquement les tweets correspondant à la règle. Dans les concepts, les correspondances sont basées sur une méthode de "meilleure correspondance". La méthode de meilleure correspondance détecte lorsqu'un texte correspondant à un concept et recouvre un texte correspondant à un autre concept. Nous utilisons une règle de classification qui identifie les termes simples ou les chaînes de caractères avec les règles CLASSIFIER, voir l’annexe 4.

Lorsque nous prenons la journée du 5 janvier, cinq concepts sont identifiés comme les plus récurrents dans les contenus diffusés par ordre décroissant :

- Activité de l’opposition
- Indicateurs de diffusion d’image

- Indicateurs de mouvements
- Actes violents
- Activités des forces ukrainiennes

Le 19 janvier, 8 concepts reviennent, voir figure 35

- Activités des forces de l'ordre
- Activités des forces ukrainiennes
- Activités de l'opposition
- Actes violents
- Indicateurs de diffusion
- Armement
- Malveillance
- Mode opératoire

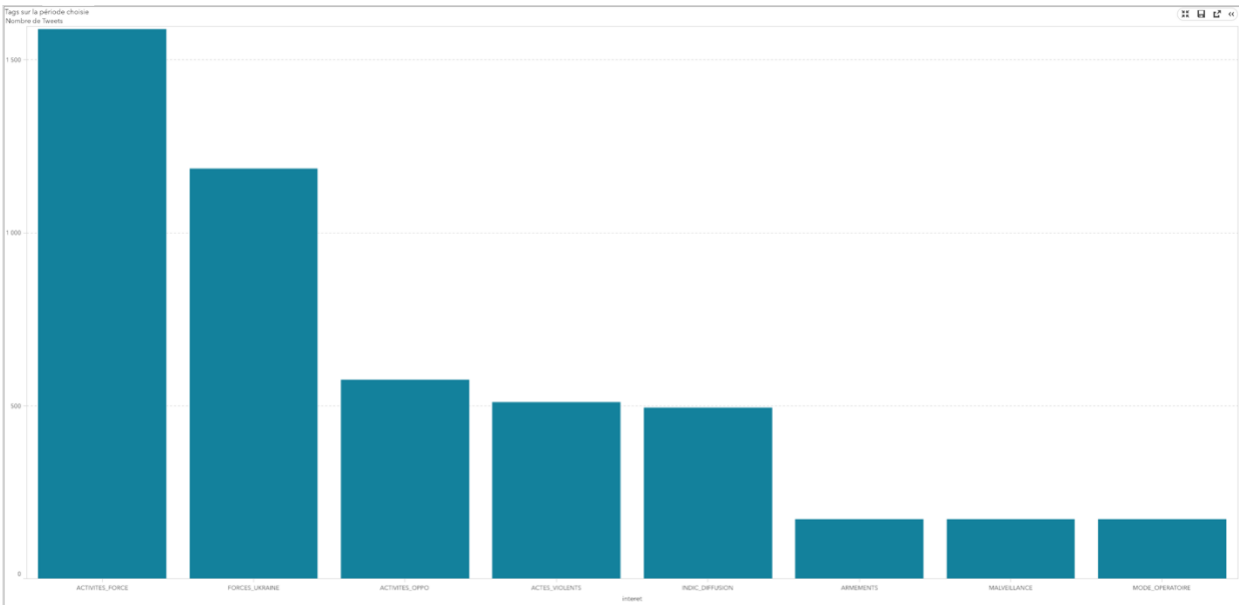


Figure 35 : Liste des concepts du 19 janvier

Le 20 février, 9 concepts reviennent, voir figure 36 :

- Activités des forces ukrainiennes
- Malveillance
- Actes Violents
- Activités des forces de l'ordre
- Indicateur de diffusion
- Activités des forces pro-russes
- Injonctions
- Armement
- Mode opératoire

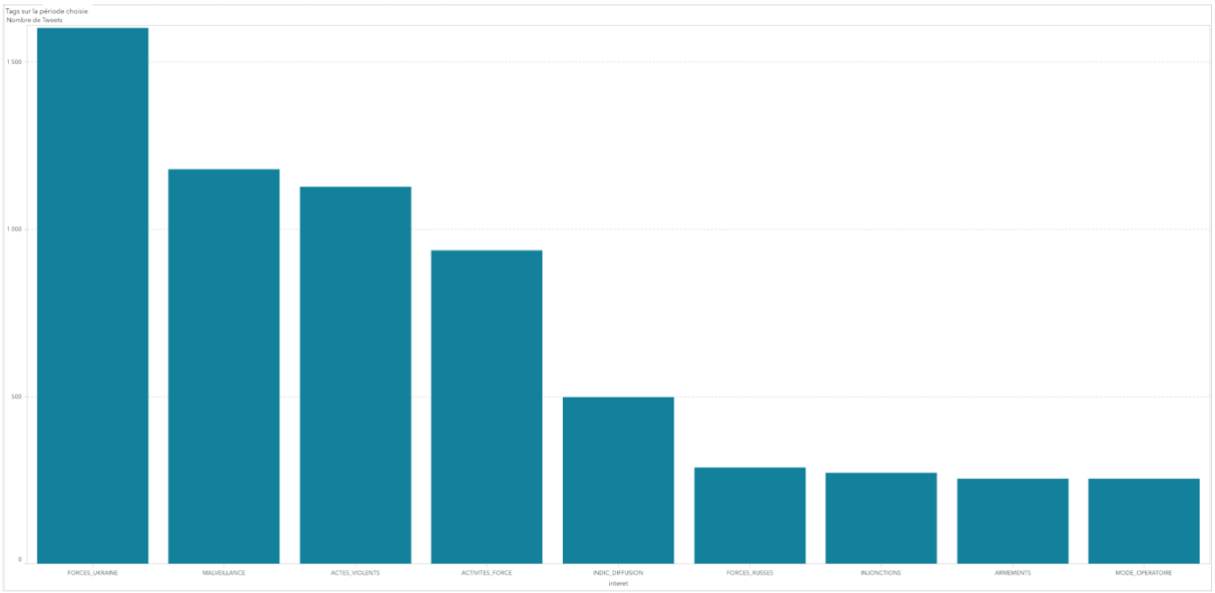


Figure 36 : Liste des concepts du 20 février

L'analyse sémantique permet de comprendre de quoi parlait les émetteurs de tweets pendant les journées d'intérêt détectées grâce à l'analyse sémantique. Il ressort que les sujets abordés les 5, 19 janvier et le 20 février sont cohérents avec la nature des évènements qui se sont déroulés à ces dates.

Nous avons ensuite cherché des mots particuliers pour voir s'ils nous permettaient de suivre les évènements. En cherchant les occurrences du mot раненых (blessés) nous obtenons le graphique suivant :

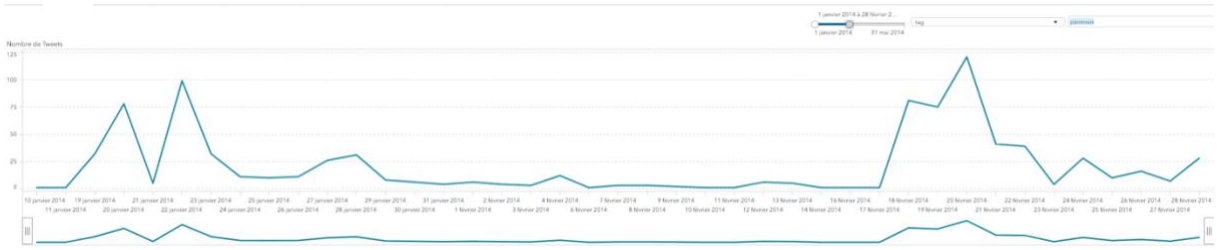


Figure 37 : Occurrences du mot « blessés » sur les mois de janvier et février

Ce graphique met en avant les dates suivantes :

- 20 - 22 janvier : violents affrontements sur la rue Grushevskogo
- 18 février – 20 février : 88 à 103 civils et 13 policiers perdent la vie.

Une autre approche consiste à découvrir ce que disent les tweets à caractères informatifs. Pour cela nous utilisons un procédé permettant la découverte automatique des tweets contenant un sujet, un verbe, un objet (SVO). La plateforme SAS permet autre autres la catégorisation automatique des mots en catégorie telles que : Nom, Verbe, Adjectif, Adverbe, Conjonction Nombre, Déterminant, Interjection, Quantificateur interrogatif, Nom propre.

Séparateur ou ponctuation, etc. Nous avons procédé à un assemblage de commutation consistant à regrouper les éléments constitutifs de la même catégorie grammaticale. De ce fait les catégories sujet et objet peuvent être un nom, un pronom, un infinitif ou une proposition. Seule la catégorie verbe est unique.

Sur la période du 10 au 20 février 2014, la volumétrie nous indique deux moments : une séquence de faible diffusion entre le 10 et 17 suivie d'une séquence de forte activité entre le 17 et le 20, voir figure 38.

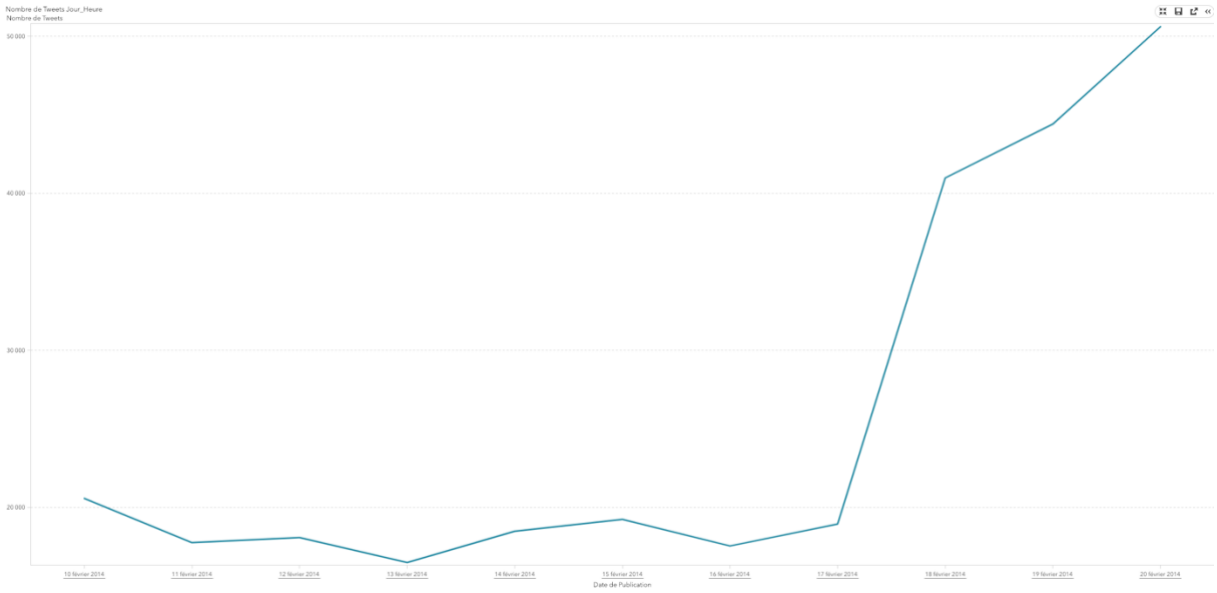


Figure 38 : Suivi du volume d'émission du 10 au 17 février

Si l'on regarde les tweets ayant une structure SVO sur la séquence du 10 au 17 février, les cinq messages SVO les plus diffusés étaient :

- Вильнюс станет похож на Киев. Атмосферой Евромайдана. Авторская колонка редактора "NR Baltija" : Vilnius commence à ressembler à Kiev. Atmosphère Euromaidan. Editorial du rédacteur en chef de "NR Baltija"
- в киеве свозят танки : les chars sont amenés à Kiev
- Киев потратит на аренду площади на выставке недвижимости в Каннах 62 тысячи евро : Kiev consacrera 62 000 euros à la location stand au salon de l'immobilier de Cannes
- Мое новое достижение `Горняк`. Попробуй превзойти меня в The Tribez для #iPad! http://t.co/OuTfFSQj2P #ipadgames, #gameinsight : Ma nouvelle réalisation `Miner`. Essayez de me battre dans The Tribez pour #iPad! http://t.co/OuTfFSQj2P #ipadgames, #gameinsigh
- Литва отмечает День восстановления независимости / В Вильнюсе - огромный флаг, костры и призыв к единению общества http://t.co/37eU9qA1Nn : La Lituanie célèbre le Jour de la restauration de l'indépendance / Vilnius - un drapeau immense, des feux de joie et un appel à l'unité de la communauté http://t.co/37eU9qA1Nn

Un seul sujet porte sur l'actualité locale. Le reste porte sur des sujets de géopolitique internationale (2), un sujet économique, et une publicité. De plus les sujets sont distribués de façon équilibrée. On constate une grande diversité de sujets, voir figure 39.

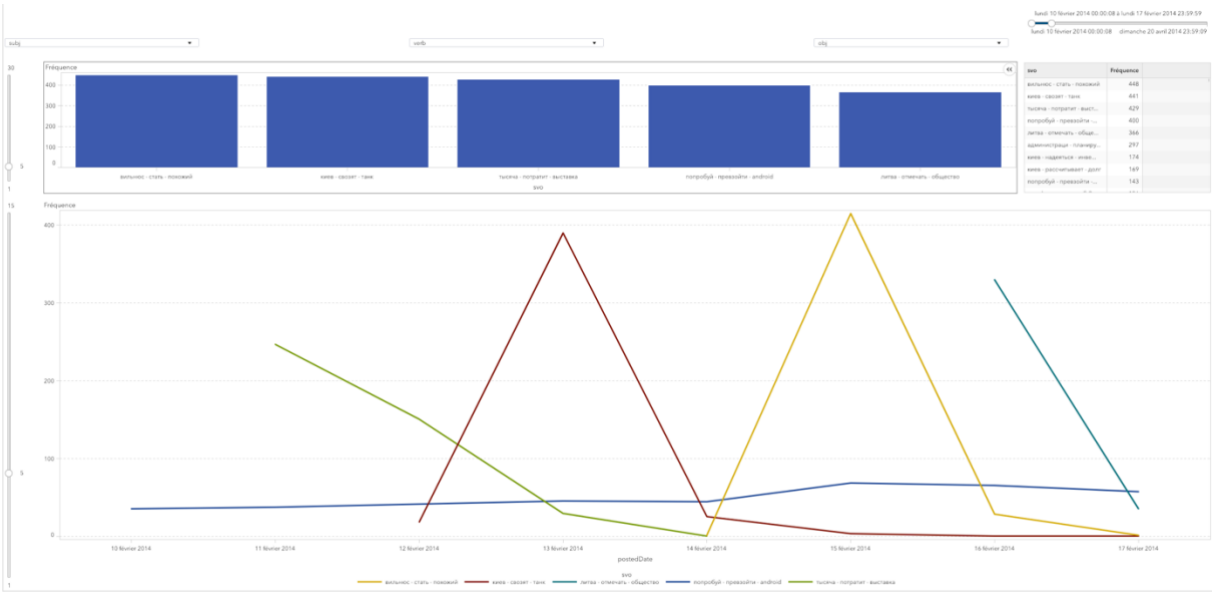


Figure 39 : Répartition des tweets ayant un format sujet-verbe-objet du 10 au 17 février 2014

Sur la période du 17 au 20 février : les sujets sont radicalement différents à l'exception de la publicité diffusée par le même automate, voir figure 40.

- L'unité " Berkut » a attaqué sans succès le Maidan et a perdu "beaucoup" de combattants faits prisonniers
- Мое новое достижение `Горняк`. Попробуй превзойти меня в The Tribez для #iPad! http://t.co/OuTfFSQj2P #ipadgames, #gameinsight : Ma nouvelle réalisation `Miner`. Essayez de me battre dans The Tribez pour #iPad! http://t.co/OuTfFSQj2P #ipadgames, #gameinsigh
- Variété de tweets d'alertes lancés par euromaidan
- Верховная Рада приняла решение работать без перерыва до окончания кризиса : Le parlement décide de travailler sans relâche jusqu'à la résolution de la crise
- Правительство Украины закрыло Киев для въезда http://t.co/tLOKDgCk4A : Le gouvernement ukrainien a fermé les accès à Kiev

Açgrtomif,xn =kwxnv k domine tous les autres. On constate une concentration thématique, indicateur de crise.

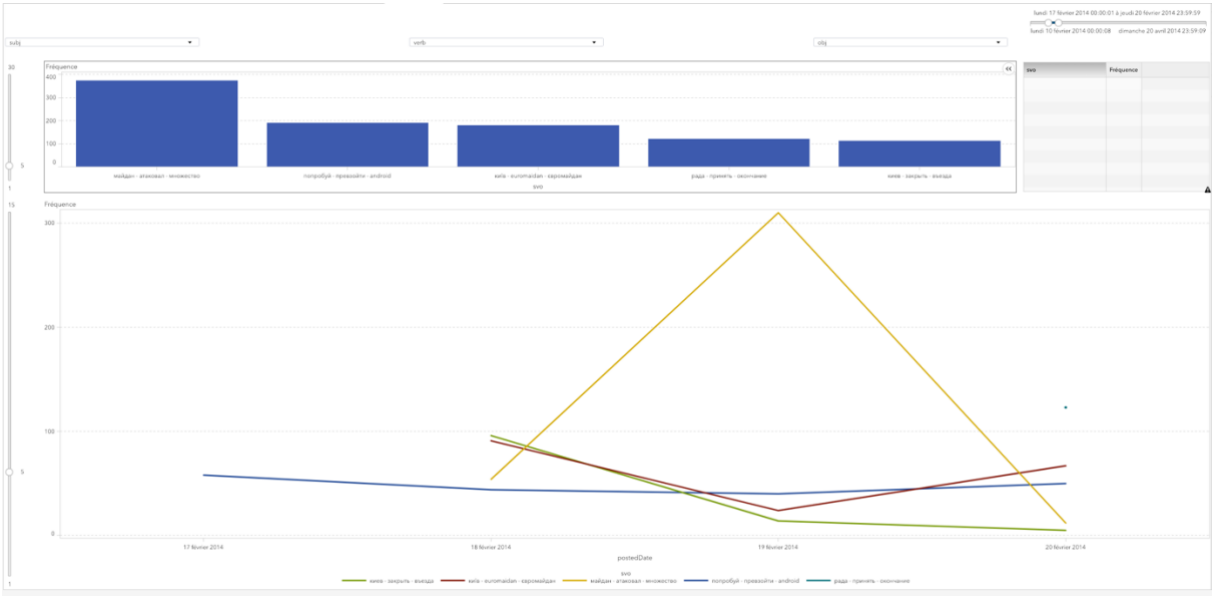


Figure 40 : Répartition des tweets ayant un format sujet-verbe-objet du 17 au 20 février 2014

Sur la journée du 20 février les tweets ayant une structure SVO sont par ordre décroissant :

- Верховная Рада приняла решение работать без перерыва до окончания кризиса : Le parlement décide de travailler sans relâche jusqu'à la résolution de la crise
- Путин отправил в Киев Лукина : Poutine a envoyé Lukin à Kiev
- Путин направил своего представителя в Киев : Poutine a envoyé son repésentant à Kiev
- Путин отправил лукина в качестве посредника от росси : Poutine a envoyé Lukin comme intermédiaire de la Russie
- верховна рада постановила вывести войска из киева : le parlement décide le retrait des troupes de Kiev
- Путин отправил в Киев Лукина в качестве посредника от России: Представитель российского омбудсмена Наталья Мирза в беседе с корреспон... : Poutine a envoyé Lukin à Kiev en tant que médiateur de la Russie: la représentante du médiateur russe Natalia Mirza dans un entretien avec le correspondant …

- верховна рада украины проголосовала за прекращение огня и выведение войска из киева : Le parlement a voté pour le cessez-le-feu et le retrait des troupes de Kiev

On constate la même distribution des sources et des volumes que lors de la journée de haute intensité du 19 janvier et la même concentration thématique. Les sujets portent tous sur les évènements en cours. Et un sujet domine significativement les autres, voir figure 41.

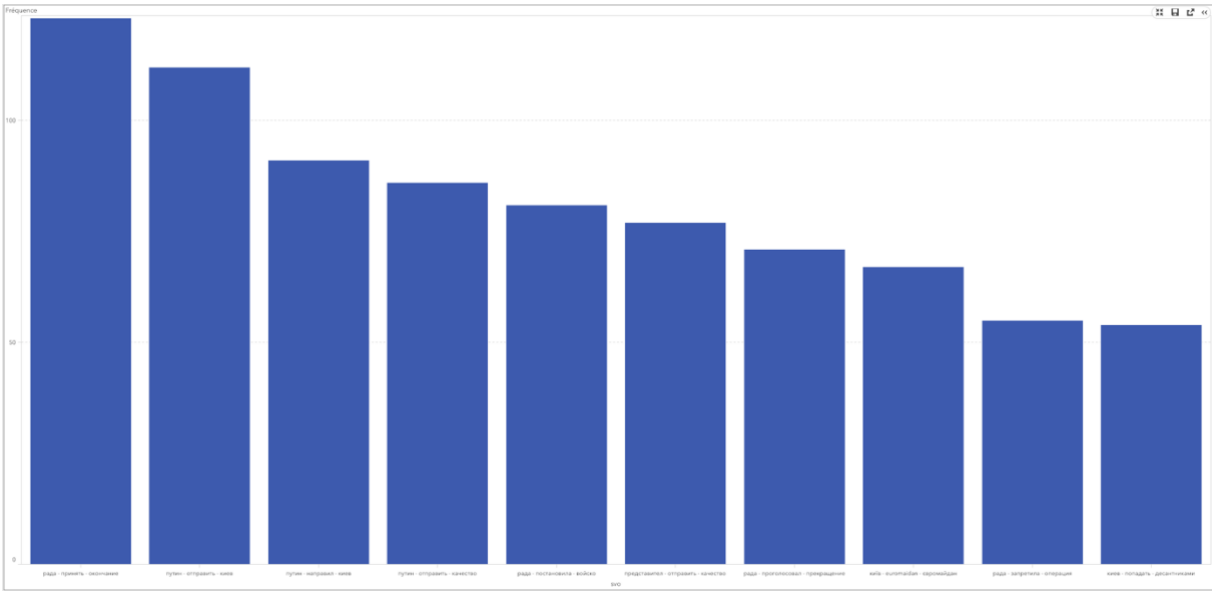


Figure 41 : Triplets sujet-verbe-objet classé en volume le 19 janvier 2014

Si l'on reprend la première phase, celle des grands rassemblements dominicaux jusqu'au janvier 2014, nous avons les 5 et 12 janvier avant les lois anti-manifestations et les 19 et 26 janvier après. L'analyse statistique nous montre que les volumes sont en constante augmentation sur tout le mois de janvier avec un pic le mercredi 22 janvier annoncé par une forte progression amorcée dès le 18 janvier, voir figure 42.

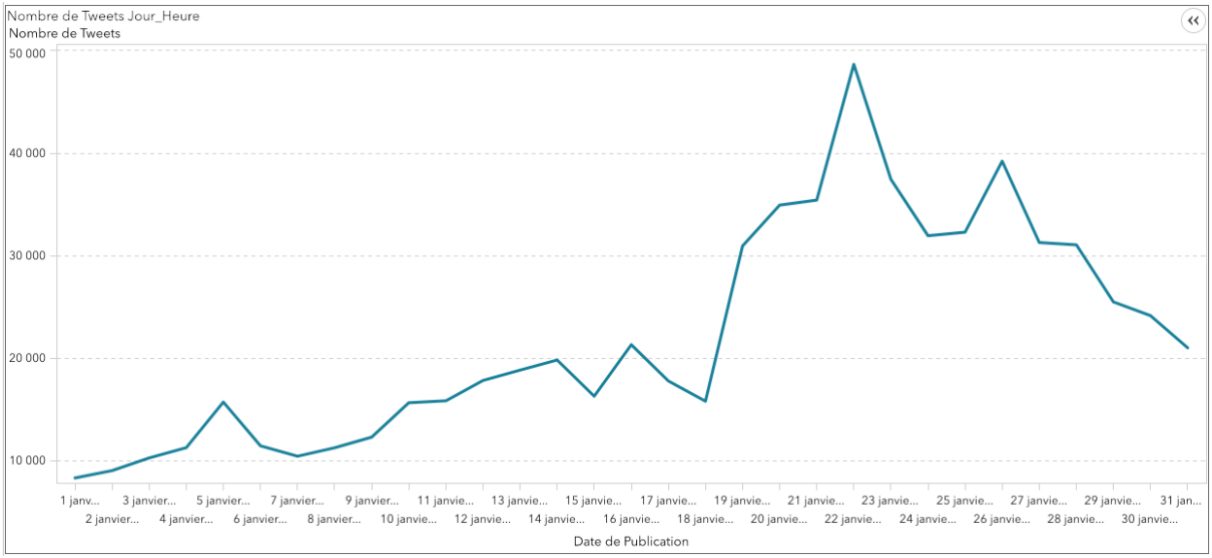


Figure 42 : Nombre de tweets par jour au mois de janvier 2014

Plus on observe des évènements sur une longue période plus l'analyse statistique permet d'isoler a posteriori les évènements majeurs. Ainsi sur une période de 5 mois allant de janvier à mai 2014 chaque pic correspond à évènement significatif du conflit.

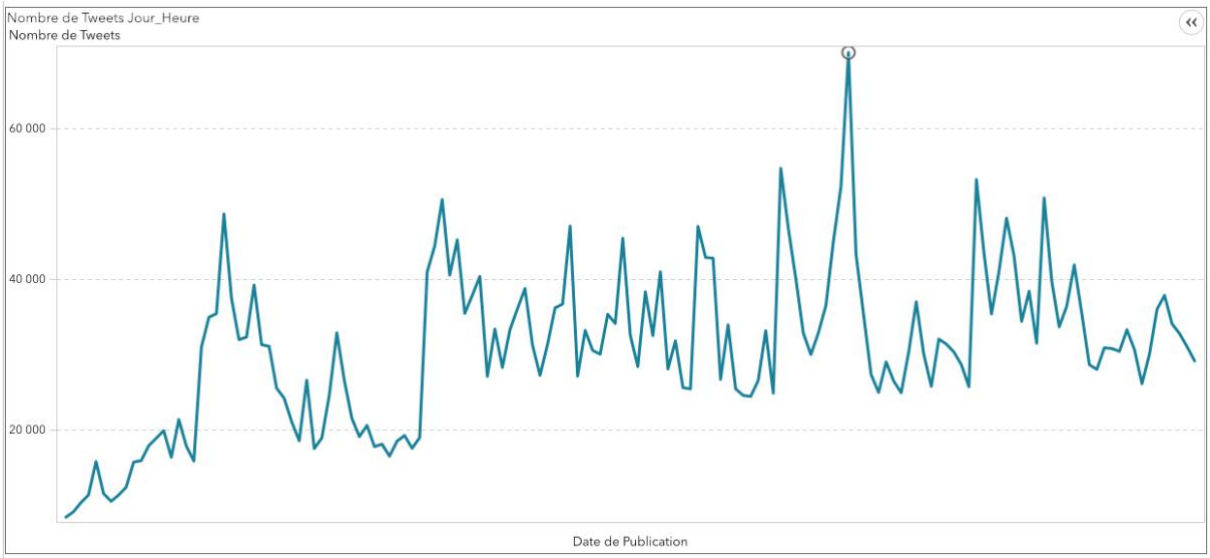


Figure 43 : Nombre de tweets par jour des mois de janvier à mai 2014

Nous avons effectué une autre approche. Compte tenu du fait que les tweets sont des messages très courts, ils sont propices aux abréviations et au contenu réduit au minimum. Alors au lieu d'une séquence complète sujet-verbe-complément nous avons regardé ce que donnerait une séquence composée uniquement d'un verbe. Cependant, afin de ne pas être submergé par les tweets à caractères commerciaux nous avons mis un dictionnaire de 246 verbes liés à des situations d'affrontement, voir annexe 4.

Le 5 janvier on relève des verbes qui relève du contrôle de manifestation, voir figure 44.

провести	tenir
одолеть	battre
прекратить	arrêter
нанести	appliquer
избит	tabasser
рушит	détruire
сбежать	fuir
гонять	conduire
защищать	protéger
мешать	interférer
остановить	arrêter
побить	battre

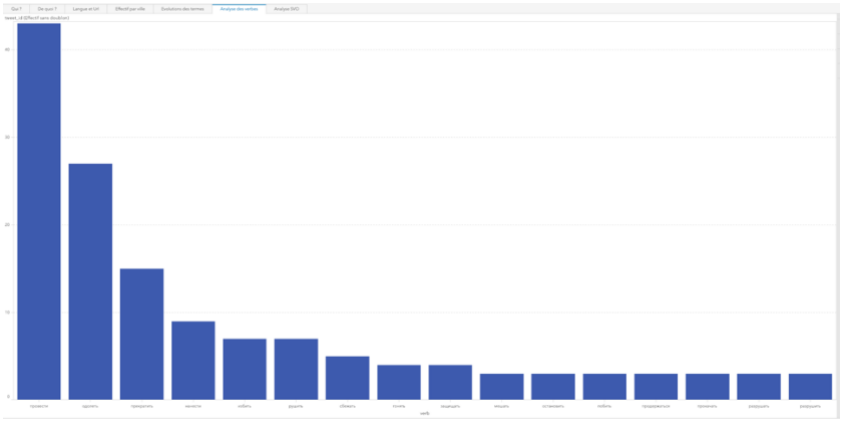


Figure 44 : Liste des verbes d'action du 5 janvier, classés par volumétrie

Le 19 janvier on relève des verbes en lien avec le maintien de l'ordre anti-émeute, voir figure 45.

штурмовать	prendre d'assaut
провести	tenir
прекратить	Faire cesser
избит	battre
остановить	arrêter
рушит	écrouler
мешать	interférer
защищать	protéger
поддаваться	succomber
избивать	tabasser
освободить	libérer
расстрелять	mitrailler

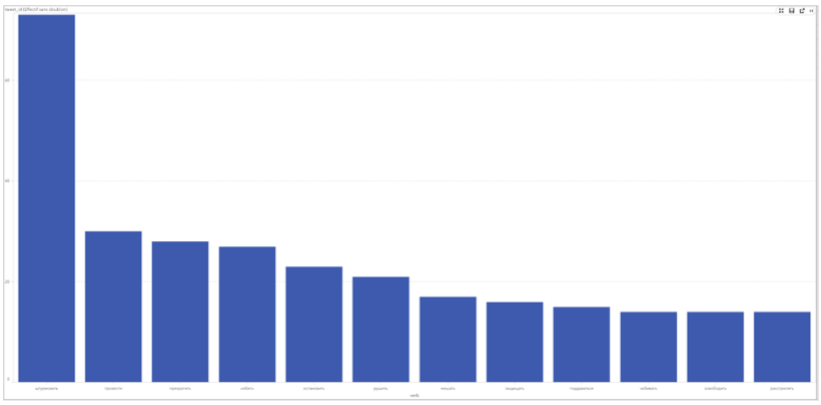


Figure 45 : Liste de verbes d'action du 19 janvier, classés par volumétrie

Le 20 février on constate on relève des verbes qui sont du ressort du conflit armé :

прекратить	faire cesser
остановить	arrêter
провести	tenir
защищать	protéger
отключить	désactiver
штурмовать	prendre d'assaut
расстрелять	mitrailler
расстреливать	mitrailler
освободить	libérer
избит	tabasser

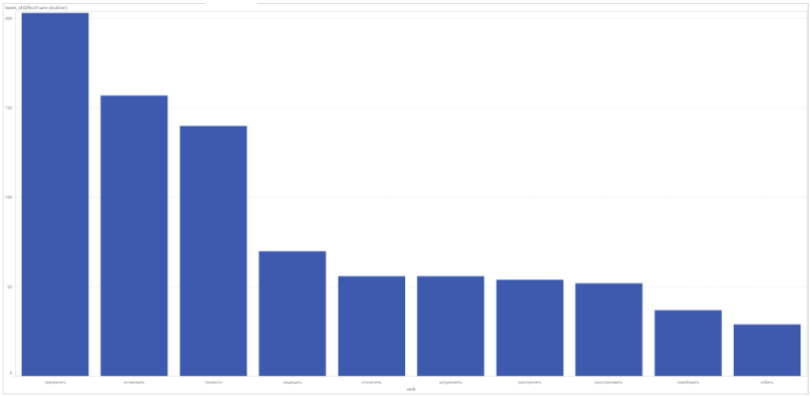


Figure 46 : Liste des verbes d'action du 20 février, classés par volumétrie

On constate que par rapport au 5 janvier, les journées du 19 janvier et du 20 février font toutes deux ressortir des verbes de violence aggravée tels que : prendre d'assaut, mitrailler, succomber. Cette rapide analyse des verbes de combat permet de nouveau de distinguer une manifestation ordinaire comme celle du 5 janvier d'affrontements extraordinaires tels que le 19 janvier ou le 20 février.

Même lors de conflit de plus haute intensité la détection des verbes d'actions pour comprendre l'évènement est révélatrice.

Au mois d'avril deux dates ressortent : le 6 avril et le 15 avril

Figure 47 : Nombre de tweets par jour de janvier à mai 2014

6 avril 2014

пытать	torturer
уничтожать	détruire
провести	tenir
освободить	libérer
штурмовать	prendre d'assaut
отстаивать	défendre
остановить	arrêter
защищать	protéger
продержаться	tenir bon
прекратить	faire cesser

15 avril 2014

штурмовать	prendre d'assaut
остановить	arrêter
освободить	libération
провести	tenir
расстреливать	tirer
восставать	rebeller
прекратить	arrêter
расстрелять	tirer
избит	tabasser
нанести	porter un coup

6.4. Analyse relationnelle

L'étude des données dans les réseaux sociaux implique évidemment l'utilisation des données relationnelles entre les acteurs. Cependant il y a un pas entre afficher massivement des liens, des méga-clusters communautaires comme le permettent certains outils de data visualisation et faire une analyse desdits liens.

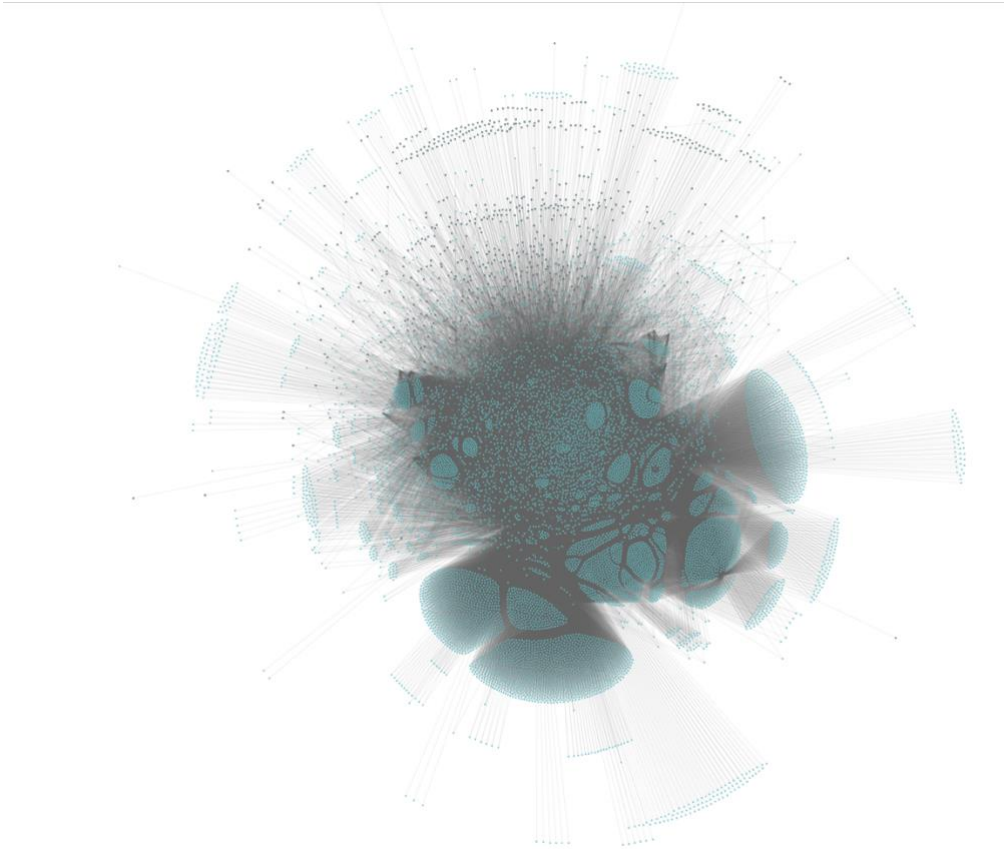


Figure 48 : Réseau des communautés des tweets

L'outil d'analyse relationnelle, au-delà de l'affichage, permet d'explorer les liens entre des personnes et/ou des thèmes contenus dans les données. Par exemple nous allons explorer les personnes exprimant leur opposition au mouvement révolutionnaire. Pour cela nous avons sélectionné les personnes employant le hashtag antimaidan en russe soit #антимайдан.

L'outil d'analyse visuelle nous permet d'afficher le réseau des hashtags employés par les utilisateurs de ce critère de sélection initiale.

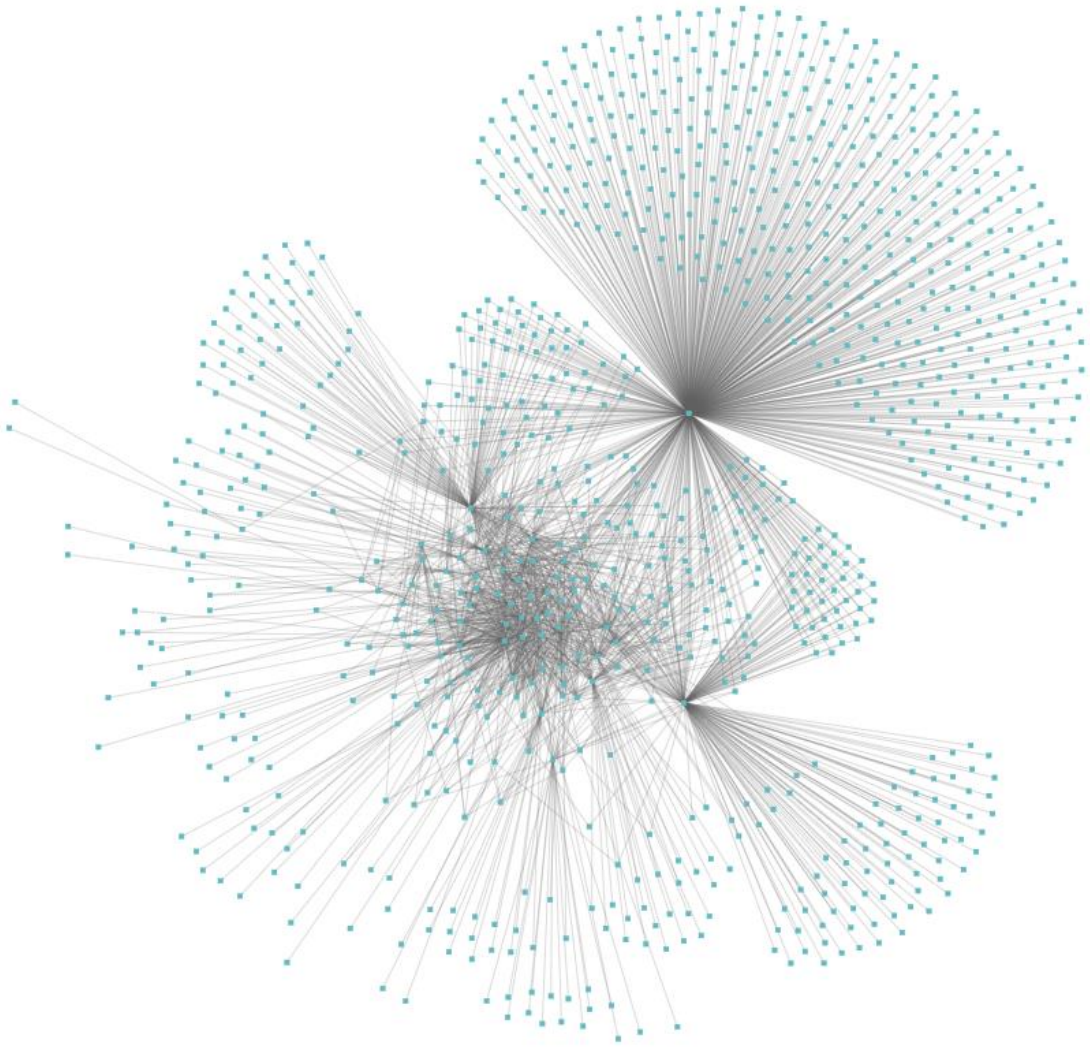


Figure 49 : Utilisateurs du hashtag #антимайдан (antimaidan)

Parmi les utilisateurs du hashtag #антимайдан on remarque trois principaux émetteurs qui utilisent le #антимайдан, voir figure 40 :

- Антимайдан (Antimaidan) ;
- Most Popular Person (personne la plus populaire) ;
- Мы Не Майдан (Nous ne sommes pas Maidan).

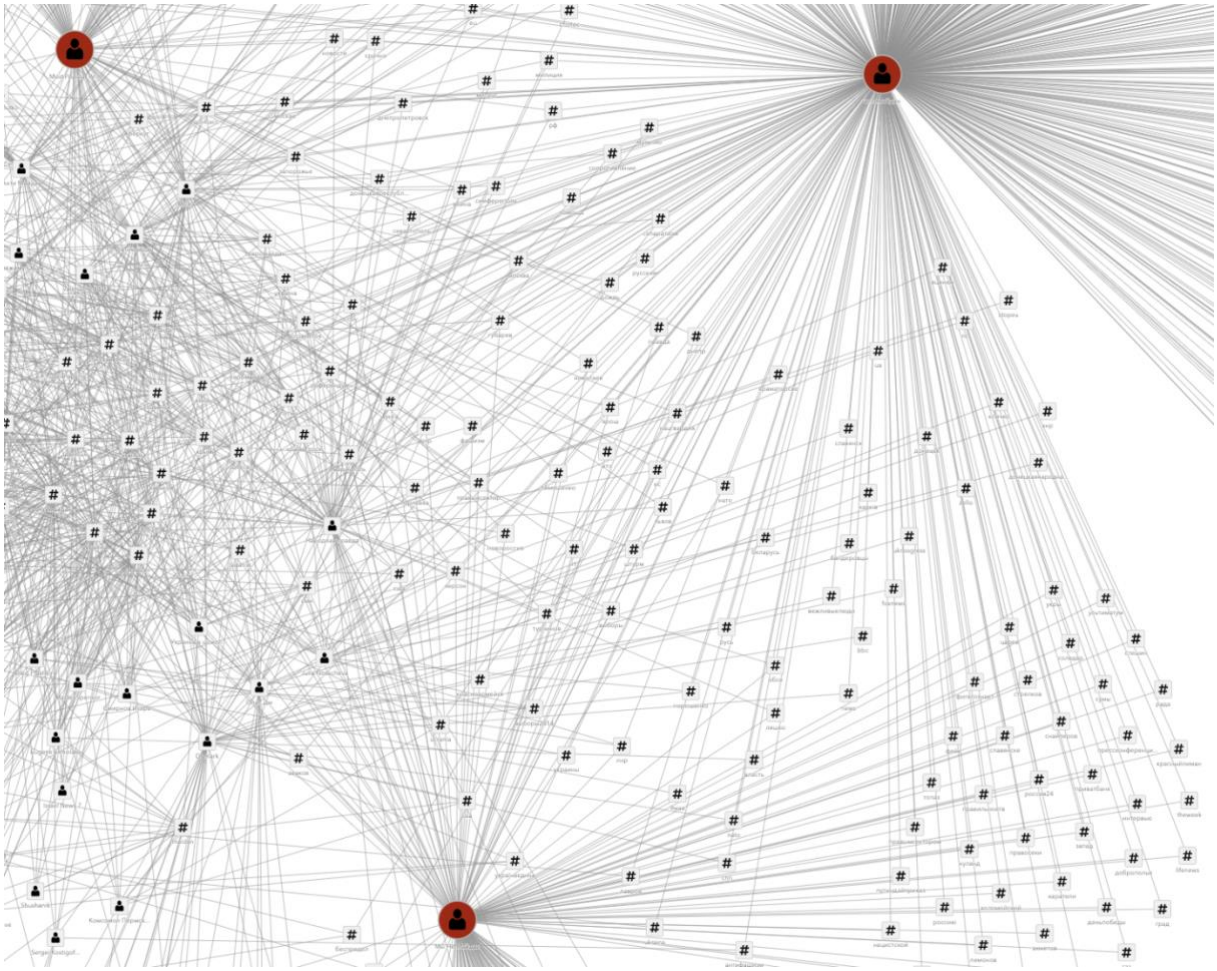


Figure 50 : Trois principaux utilisateurs du hashtag #антимайдан (antimaidan)

Là où l'outil d'analyse relationnelle va apporter sa plus grande plus-value c'est dans la démarche d'investigation, de concentration du point focal sur un élément en particulier plus que sur l'observation de la masse.

Lorsque nous zoomons sur les hashtags employés par le compte Антимайдан (Antimaidan) on voit apparaître des hashtags très polarisants compte tenue de l'histoire soviétique en générale et de l'Ukraine en particulier et du fait de la participation de partis d'extrême droite à la coalition révolutionnaire, c'est-à-dire les hashtags portant sur le nazisme. Au-delà d'une énième démonstration de la loi de Godwin selon laquelle : « *Plus une discussion en ligne dure longtemps, plus la probabilité d'y trouver une comparaison impliquant les nazis ou Adolf Hitler s'approche de 1.* » (Wiktionnaire, 2019). Les nazis sont l'ennemi ultime de la nation ukrainienne et de tous les pays de l'espace post-soviétique, leur comparer un adversaire politique est un signe fort. Il s'agit clairement d'une polarisation du discours de certains protagonistes au conflit.

Lorsqu'on ajoute dans le réseau les références au fascisme ou au nazisme on peut grâce à l'analyse relationnelle identifier qui dans la communauté du compte Antimaidan exprime les opinions les plus polarisées sur les évènements en cours.

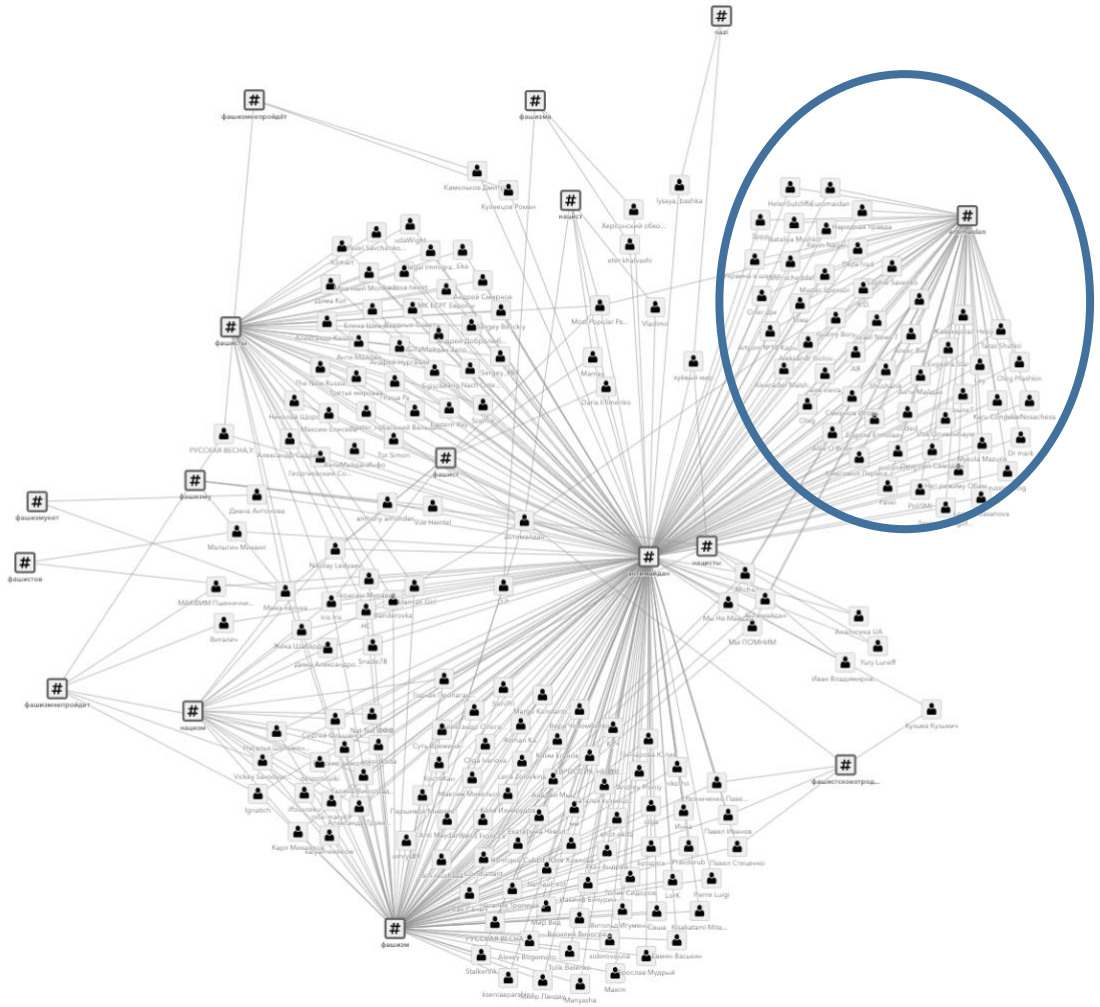


Figure 51 : Communauté faisant référence au nazisme et au fascisme

Mis à part les personnes dans le cercle bleu, toutes les autres font à un moment donné une référence au nazisme ou au fascisme.

6.5. Conclusion

Le dimanche 5 janvier constitue le 6ème dimanche consécutif de rassemblement et l'étude tant des statistiques que de la sémantique ne fait ressortir aucun élément particulier. En revanche le dimanche 19 janvier est le premier dimanche de manifestation après le vote de lois répressives. On constate un comportement d'émission différent tant du point de vue des sources que des sujets. Enfin l'étude de la journée du 20 février vient confirmer que les aspects caractéristiques d'une journée de haute intensité :

- Augmentation du volume d'émission
- Existence de plusieurs pics de retweets au cours de la journée
- Présence essentiellement de citoyens et de médias parmi les sources
- Sujet portant majoritairement sur la confrontation entre forces de l'ordre et manifestants
- Augmentation du nombre de sujets mentionnant les évènements

La détection de l'ensemble de ces critères est automatisable par une machine animée par une intelligence artificielle.

L'outil permet une analyse rapide en mémoire de données de toutes tailles. Les visualisations contribuent à des analyses descriptives, prédictives et normatives. Pour cela, l'outil doit permettre d'interroger les données à partir d'un ensemble de modes d'affichage. Les données multidimensionnelles telles que des tweets doivent être fractionnées au moyen de filtres à n'importe quel niveau de leur hiérarchie. Ces hiérarchies pour être explorées doivent être créées à la volée et inclure des niveaux extensibles et réductibles.

Au résultat, les statistiques descriptives visualisables donnent une idée globale d'un mouvement social, tout en permettant l'identification automatique des sous-évènements ou performances réalisées au cours dudit évènement afin de mettre en œuvre un « protest event analysis ». Par ailleurs, l'outil permet de détecter les évènements clefs, les points de rupture notamment grâce à l'analyse sémantique. En effet, tous les sous-évènements ne se valent pas. Il est donc essentiel de pouvoir isoler les articulations signalant un changement de direction ou de routine des manifestants que cela soit en termes de répertoire d'action collective ou de polarisation du/des discours.

La méthodologie déployée pour nos travaux est une approche séquentielle :

1 Recherche de ruptures comportementales, détection d'événement au moyen de statistiques d'émission, notamment par la méthode DETEVEN décrite en chapitre 4.
2 Compréhension d'événements à partir des centres d'intérêts mis en dictionnaires grâce aux outils sémantiques.
3 Investigation pour identifier les acteurs d'intérêts à partir d'un comportement : compte dont la majorité des tweets sont massivement retweetés, à partir d'un contenu : polarisation des propos.
4 Identification des bots qui manipulent les médias sociaux sur la base de la mise en place d'alertes.

Le suivi des réseaux sociaux en situation de crise au moyen d'une plateforme analytique est un changement de paradigme capacitaire pour des forces de l'ordre, une armée, un État qu'il s'agisse d'une crise sur son territoire ou à l'étranger.

Avec un média comme Twitter, l'information sur un évènement est disponible immédiatement. Il n'y a pas de délai d'impression ou de montage avant diffusion. Il est très compliqué d'appliquer une censure à la plateforme étant la propriété d'une société américaine.

L'information circule sans délai, l'évènement est immédiatement diffusé renforçant son impact sur les faits à venir. L'utilisateur observe l'évènement et transmet immédiatement son émotion son indignation. Dans le cadre d'une manifestation par exemple, une exaction policière peut être diffusée en direct et entrainer un afflux de manifestant en quête de représailles à un point donné renforçant le potentiel d'émeute.

Conclusion de la deuxième partie

Dans cette partie nous avons montré comment la détection d'évènement est un sujet d'intérêt majeur pour suivre l'actualité et pour faire du renseignement. Cependant, les méthodes issues des médias traditionnels ne sont pas intégralement réplicables en l'état sur les médias sociaux. Ces derniers remplissent tous les critères du big data : grand volume de données, variété des sujets, vitesse de diffusion, valeur inégale, véracité parfois douteuse, ce qui complique significativement la détection de faits qui peuvent être des évènements. Ils disposent par contre d'une qualité unique, leur contenu étant généré par leurs utilisateurs. Même pendant les heures les plus noires d'un conflit leur accès n'est que très rarement coupé, et toujours de façon temporaire. Ils sont potentiellement incensurables. Chaque utilisateur, devenu capteur social, peut annoncer un évènement dont il est témoin. Les services de renseignement doivent avoir la capacité de détecter ces témoignages. Pour cela il faut mettre en œuvre une méthode adaptée aux contraintes des médias sociaux.

La détection d'évènement dans les médias sociaux est largement documentée, elle fait partie des recherches sur les tendances au même titre que le suivi d'évènement, et l'interprétation. Elle est considérée à juste titre comme la phase la plus importante par Seifikar et Farzi dans leur revue des algorithmes de suivi dans les réseaux sociaux. Dans cette revue ils distinguent quatre dimensions à la détection : thématique (basée sur le contenu textuel), temporelle (horodatage du contenu), spatial (coordonnées géographiques), relationnelle (liens entre les documents) (Seifikar et Farzi, op. ci., 2019). Notre méthodologie DETEVEN est une innovation de ces approches. Dans DETEVEN la détection est : thématique et spatiale, elle repose sur la détection de toponymes texte et non de coordonnées géographiques ; elle est temporelle, par la détection d'anomalie de volumétrie, et non strictement issu d'un horodatage ; et elle est relationnelle car dans le réseau de Twitter on peut agglomérer les tweets d'un évènement en remontant les liens entre utilisateurs.

En partant du principe qu'un évènement qui touche les gens est ancré dans un lieu, nous proposons la méthode DETEVEN de détection d'évènement par les toponymes. Plus un toponyme est présent dans le flux, plus il y a des chances qu'un évènement s'y déroule. Malheureusement, le suivi de la simple volumétrie ne permet de détecter que les évènements massifs et pas les signaux faibles. Nous proposons de classer les toponymes par pourcentage de croissance par rapport à une période précédente. Cette méthode a permis de détecter chaque évènement ayant lieu pendant la crise, dans n'importe quelle ville ou village, même quand il

n’est mentionné que quelques dizaines de fois dans un flux de plusieurs dizaines de milliers de tweets.

Une fois l’évènement détecté, il faut l’analyser. Pour cela il faut d’abord l’inscrire dans son contexte informationnel. Nous avons retracé la chronologie des phases de la crise ukrainienne qui est considérée comme un cas de référence dans le domaine de la guerre hybride. Pour illustrer la partie du conflit se déroulant sur les réseaux sociaux, nous avons proposé une méthode de détection des botnets qui saturent le flux pour garder un maximum de visibilité à des thématiques particulièrement clivantes, et fausses. Ces étapes de nettoyage des données est un préliminaire essentiel à l’analyse pour le renseignement de situation.

Ensuite nous avons proposé une analyse d’un théâtre d’opération connecté (TOC). Quelles que soient les opérations militaires, officielles et officieuses, en cours sur le champ de bataille, le TOC implique toutes les parties prenantes et les emmène à l’affrontement sur d’autres domaines comme les opinions publiques. Nous avons proposé un ensemble de mesures permettant de caractériser un TOC telles que pourcentage de progression d’ouvertures de comptes, volume d’émissions quotidienne, langues employées, etc. De nouveau nous avons montré le rôle de révélateur d’évènement des toponymes dans le suivi d’activité d’une ville quelle que soit la taille de la ville. Nous avons également montré qu’une façon d’identifier les sources primaires était de chercher les tweets mentionnant les 5 sens à la première personne du singulier. Le dernier chapitre illustre l’apport de l’analytique. Nous avons passé en revue les utilisations de l’analyse statistique, sémantique et relationnelle et de leurs outils de visualisation des données. Au travers du conflit ukrainien, nous avons illustré le fonctionnement de ces outils qui contribuent au suivi de situation et au renseignement sur un TOC.

Le principe de la guerre hybride étant la permanence du conflit, dans la troisième et dernière partie de nos travaux, nous allons appliquer les méthodologies décrites pour travailler sur des opérations d’influence, le déploiement d’une solution de police guidée par le renseignement analytique et l’impact de cette guerre sur la maîtrise de l’information.

Troisième partie : De la détection des évènements pour la « maitrise de l'information »

Introduction

Cette troisième partie de nos travaux a pour but de montrer comment la même combinaison de logiciel, d'algorithme et de méthodologie qui peut être employée sur un théâtre d'opération connecté peut également contribuer à sécuriser notre société. La capacité à détecter au moyen de plateformes analytiques et d'intelligence artificielle des évènements de nature à changer le cours d'une situation de conflit voire de l'histoire est tout aussi pertinente sur le territoire national. La guerre hybride légitime les opérations sur la base de soutien de l'adversaire. Dans le domaine de l'influence sur une opinion publique, la perturbation d'élections et la diffusion de fausses informations sont les méthodes de prédilection. Dans le premier chapitre nous illustreront les capacités qu'il est possible de mettre en œuvre, au travers des plateformes définies dans la deuxième partie, pour surveiller si une tentative d'influence à lieu sur une campagne électorale. Nous réaliserons dans un second temps une analyse d'une fake news. Dans le second chapitre nous distingueront les fantasmes de la police prédictive de l'approche pratique de la police guidée par le renseignement. Aujourd'hui la police ne fait qu'une utilisation minime des données dont elle dispose. Nous expliquerons comment l'exploitation de ces données au moyen d'une plateforme analytique révolutionnerait la façon d'opérer et permettrait une plus grande efficacité et efficience. Enfin après avoir étudié les opérations adverses (influence et fake news), illustré l'apport de l'analytique pour la sécurité intérieure, nous élèverons le débat pour inscrire la sécurisation d'une société par la maîtrise de l'information. Nous montrerons comment cette maîtrise de l'information, facteur de sécurité et de résilience, repose sur la capacité de l'individu d'acquérir des capacités et des compétences. Pour cela nous mettrons en évidence pourquoi il faut qu'il y ait une volonté politique d'inscrire l'éducation aux médias et à l'information comme priorité nationale et la rendre disponible tout

au long de la vie. Enfin nous appellerons l'attention sur le fait que cette maîtrise n'est rien sans une capacité à agir sur l'internet. Cette révolution de l'accès à l'information est l'objet de nombreuses luttes qu'il s'agisse de sa gouvernance ou de sa neutralité. Les enjeux sont énormes pas seulement d'un point de vue financier, mais surtout du point de vue de l'impact qu'il a sur la société dans son ensemble.

7. Chapitre 7 : Les cas d'usage opérationnels

7.1. Introduction

Le développement de la solution DETEVEN s'est fait à la fois dans un contexte de recherche, mais aussi dans un contexte industriel avec la société OAK BRANCH. L'objectif de ce chapitre est d'illustrer les travaux par des applications déployées réalisées dans des environnements opérationnels. Deux projets seront présentés : une méthodologie de recherche d'influence dans un contexte électoral et une analyse de fake news. Chacune de ces études met en évidence la nécessité d'avoir des équipes formées tant en data science qu'en sciences humaines et sociales, les opérations adverses employant des techniques de ces deux domaines.

Une tentative d'influence se caractérise par la volonté d'un groupe, d'un gouvernement ou de n'importe quelle organisation d'influencer le cours d'un ou des événements afin d'obtenir ou de tendre vers un objectif précis ; ce dernier pouvant être identifié sous différentes formes. L'objet de cette analyse fait suite à de nombreux précédents dans les processus électoraux et référendums occidentaux. À cet effet, nous avons utilisé notre base de connaissance sur les manipulations ayant eu lieu et cherché à détecter la survenue de ce type d'opération ou d'action s'en approchant. La diffusion d'une fake news c'est-à-dire : « *Information fabriquée et publiée sciemment dans le but de tromper et d'inciter un tiers à croire à des mensonges ou à mettre en doute des faits vérifiables* » (Unesco, 2017) qui plus est, déjà tentée quelques années auparavant, n'est pas un succès systématique. De plus, la détecter n'est pas l'attribuer. Cependant il est possible d'en estimer l'origine grâce à une comparaison de données dans le temps. Chacune de ces études est une opportunité de déployer la méthodologie DETEVEN sur de nouvelles problématiques. Elles sont également l'occasion de concevoir de nouvelles interfaces en partenariat avec les utilisateurs finaux nous donnant un aperçu de leur méthodologie de travail.

7.2. Application sur une analyse d'influence

Après plus de vingt ans de baisse, la participation de l'électorat français aux élections européennes de 2019 a été estimée à plus de 50%, soit 8 points de plus qu'aux élections de 2014. En observant les réseaux sociaux, nous nous sommes aperçus que les élections n'étaient pas forcément le sujet de préoccupation principal des Français : le mois de mai est un mois avec beaucoup d'événements à grande médiatisation (manifestations hebdomadaires des gilets jaunes, manifestations du 1er mai, festival de Cannes, événements sportifs divers…) et le pont de l'ascension a certainement joué en la défaveur des scrutins qui tombaient en même temps. Pourtant, l'électorat français s'est davantage déplacé aux urnes pour voter.

Les principales questions auxquelles cette étude a souhaité répondre sont : est-ce qu'il y a eu une influence étrangère sur le processus électoral européen en France, si oui, à quelles fins, et avec quel impact. En croisant plusieurs types de médias, l'objectif était de voir si un message diffusé largement peut avoir un impact significatif (retweets de masse, ou diffusion amplifiée artificiellement) sur l'audience cible. Au travers de tous ces médias, observions-nous des moyens mécaniques artificiels de diffusion à large portée ? Identifions-nous des groupes qui conduisent des opérations d'influence ?

En nous basant sur les différentes plateformes utilisées pour diffuser des informations sur les élections européennes, nous avons décidé de partir sur une méthodologie à double axe :

- Bottom-Up (analyse transverse et agnostique de la masse d'informations pour voir si des messages coordonnés émergent grâce à une collecte large, etc.)
- Top-Down (partir d'une granularité fine comme un candidat, un parti, un message, puis identifier les vecteurs et les messages d'expression de soutiens pour remonter jusqu'à une entité plus large).

Le but de l'analyse était ainsi de voir si les deux méthodes arrivaient à converger afin de mettre en avant des liens ou des concepts de nature à caractériser une influence. En cumulant ces deux méthodes, nous souhaitions être en mesure de collecter un maximum de données, qu'il s'agisse d'articles de presse, de tweets ou encore de vidéos YouTube portant sur le thème suivi et d'effectuer grâce à notre plateforme la recherche d'opérateurs d'influence.

Nous avons cherché à identifier les éventuelles influences cherchant à inciter à voter pour une certaine liste, ou contre une autre en dehors du jeu normal électoral.

7.2.1. Méthodologie

Nous avons appliqué notre méthodologie sur des médias traditionnels (presse écrite, numérique) et sur les réseaux sociaux (notamment Twitter). Les politiciens et leurs soutiens sont présents sur différents médias pour toucher un plus grand nombre d'électeurs en diffusant sur plusieurs plateformes à la fois. À ce titre, les community managers utilisent donc une diversité de médias pour impacter un maximum de personnes en fonction des tranches d'âge et des catégories socioprofessionnelles visées (télévision, journaux, sites d'information, réseaux sociaux dont Facebook, Twitter, Instagram et YouTube). Nous avons donc décidé de porter nos recherches sur plusieurs médias pour accroitre nos chances de détecter une tentative d'influence via ces derniers.

En revanche, notre accès restreint aux données de Facebook nous a contraints à surtout nous baser essentiellement sur Twitter comme réseau social principal pour la collecte du fait d'absence de contenu significatif sur les autres médias numériques (Instagram, YouTube). Cette réserve est à nuancer par le fait d'une part que nous avons plusieurs comptes Facebook (notamment bien insérés chez les gilets jaunes) que nous suivions manuellement et d'autre part du fait qu'une opération à impact significatif aurait été visible sur plusieurs plateformes simultanément par effet de propagation cross médias.

L'objectif principal des influenceurs étrangers sur les élections européennes est de fragiliser l'Europe en tant que puissance mondiale. Pour cela, ils peuvent chercher à :

- Nuire à la cohésion de la zone euro dans son ensemble,
- Contester la politique migratoire,
- Freiner l'intégration des minorités,
- Exprimer un soutien aux groupes indépendantistes / séparatistes
- Cibler une fracture nationale (Brexit, Indépendance catalane, Flamands et Wallons, Podemos, Gilets jaunes, etc.
- Soutenir les visions souverainistes

Dans tous ces cas, les méthodes d'influence fonctionnent essentiellement en homophilie : influence dans le groupe, par le groupe pour le groupe visé. L'opérateur d'influence aura de fortes chances d'exercer à l'intérieur des communautés cibles sauf dans quelques cas spécifiques notamment l'exploitation de leaks (fuite de données) et les opérations sur Facebook, c'est sur ce vecteur – pour les réseaux sociaux – que les tentatives d'influence auront le plus de chances de sortir des groupes homophiles). Pour suivre en détail les élections européennes, il

était important de cibler différentes sources à extraire, intégrer et analyser. Ainsi, nous avons étudié principalement la presse numérique russe (RT, Sputnik...), la presse numérique française (Le Monde, Le Figaro...), mais également les réseaux sociaux (Twitter principalement et Facebook en navigation uniquement) ou encore les plateformes multimédias (YouTube et ses commentaires). À cela nous avons également rajouté des sites de dénonciation de fake news comme DisinfoVsEurope pour élargir notre spectre de recherches et d'analyse.

7.2.2. Préparation des données

- Rôle de l'analyste

Dans un premier temps, l'analyste étudie le sujet demandé pour en extraire des mots clés pertinents et pour déterminer comment s'orienteront les recherches. Dans le cas ici présent, il était important d'identifier les différents acteurs des élections européennes en France, mais aussi les médias sur lesquels baser les extractions de données. Tous ces éléments sont ensuite envoyés aux spécialistes IT pour qu'ils puissent procéder à l'extraction des données ciblées. En parallèle, l'analyste s'appuie sur les différentes méthodes d'influence étrangère connues pour augmenter son champ de recherche et ainsi permettre d'identifier les possibles similitudes de scénario avec des opérations précédemment identifiées.

Pour mener cette étude, une des premières étapes est d'identifier les 78 têtes des 34 listes qui se présentaient aux élections européennes, mais aussi les professions de foi afin de les répertorier dans un document à destination de l'équipe de data scientists. Cette base est nécessaire pour permettre au système d'assister l'analyste dans ses recherches.

- Rôle du spécialiste IT

Le travail de l'IT porte principalement sur le développement de collecteurs web adaptés à l'étude. Cela a conduit à la réalisation, en interne, d'un logiciel/script Python (voir schéma) transformant les données du web en données exploitables par la plateforme.

- YouTube : récupérer tous les commentaires des vidéos partagées (découverte en direct sur YouTube ou via partage sur d'autres réseaux sociaux) au sujet des élections
- FranceInfo : récupération des articles de la section "vrai ou fake" qui comporte des articles relatifs aux élections
- RTNews : collecte de masse de pages
- Sputnik : collecte des pages portant les tags des élections européennes

– DisinfoVsEurope : récupération d'un maximum d'articles dénonçant les fakes news concernant les élections

Les résultats sont exportés en JSON, un format fédérateur pour les différents site web de presse pour faciliter l'intégration (JSON.org, 2019). La collecte de Youtube a conduit à un export dans un format JSON plus dense qui ne peut s'inscrire dans celui des articles de presse. Twintt (twint source : https://github.com/twintproject/twint) exporte les données twitter en CSV ou JSON. Le format CSV a été choisi ici :

– collecte des tweets des 5 premiers candidats des listes les plus importantes ainsi que le compte officiel du parti politique ;
– collecte des mots clés attribués aux élections européennes ;
– collecte de compte ciblé.

L'ensemble du travail s'est porté sur le secteur français. Le contenu des articles de presse recueillis a été intégré dans la plateforme ainsi que la version originale (html) et les autres références (l'article original de la fake news par exemple). Le but est d'obtenir une masse d'informations qui sera raffinée par l'analyste au moyen la plateforme pour :

– faire émerger des regroupements (clusters) d'idées ou d'individus ;
– permettre de faire des liens entre des comptes ;
– faire apparaitre des bots.

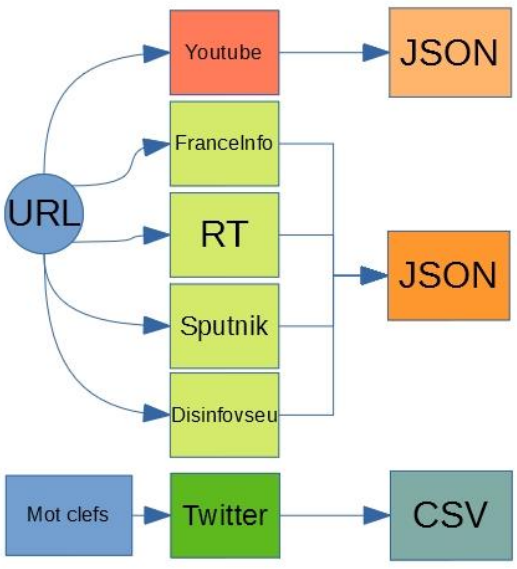


Figure 52 : Étapes préalables à l'intégration des données : recueil et conversion des données

- Rôle du Data Scientist

Le Data Scientist intervient une fois la collecte de l'IT terminée. Son rôle est de rendre les données collectées disponibles pour l'analyste en les intégrant à notre plateforme d'investigation. Son travail débute avec la récupération des fichiers de sources suivie de leur conversion en tables de données relationnelles. Il est alors possible d'importer une nouvelle entité. Une entité est créée pour les candidats, les partis politiques, les articles de presse, les tweets et les vidéos YouTube avec leurs commentaires. Il peut être utile d'enrichir certaines entités avec des informations supplémentaires comme associer à chaque candidat son compte Facebook et Twitter quand on dispose de cette information.

Il est ensuite essentiel de pouvoir lier les entités entre elles. Ainsi, pour pouvoir créer une relation entre un article et les différents candidats qu'il cite, des algorithmes de "Name Entity Recognition" sont utilisés pour extraire des entités nommées : patronymes, partis politiques ... La création de ces relations est nécessaire pour pouvoir construire le réseau des candidats. Enfin, la dernière étape consiste à personnaliser les pages utilisateurs pour chaque entité en fonction des recommandations de l'analyste.

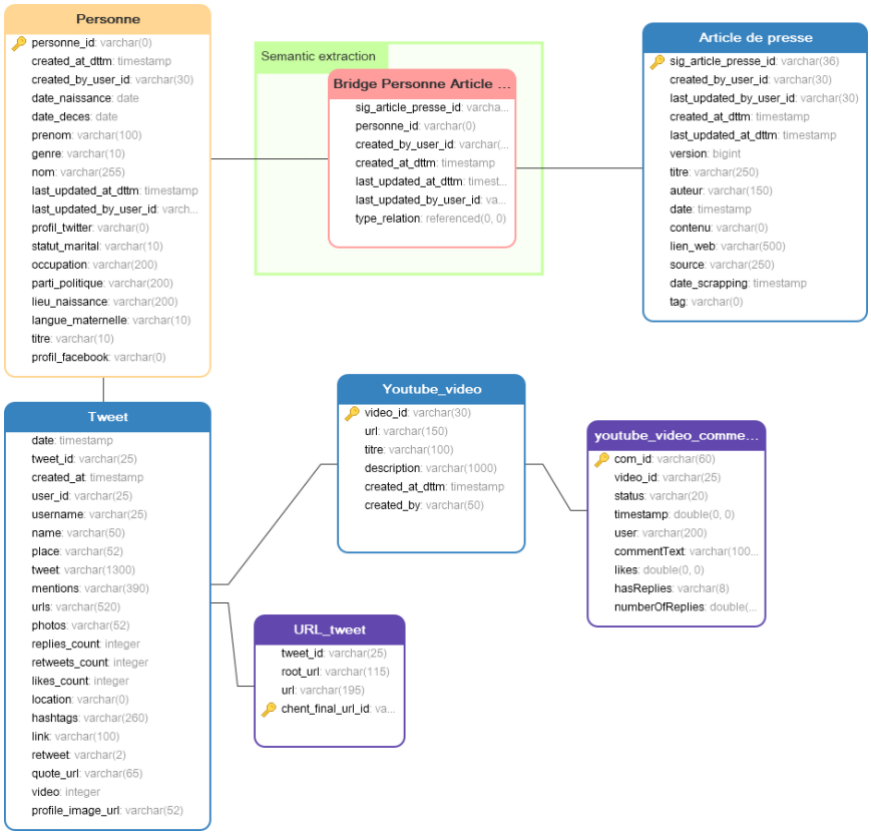


Figure 53 : Modèle de donné de l'étude

- Étape préalable à l'intégration de données : définition du modèle de donnée

  Ce modèle de donnée est totalement libre et adaptable ; il est stocké grâce à des processus d'import dans une base PostgreSQL. Une fois construit, il est également indexé par Elastic-search pour que l'analyste puisse dans une interface unique avoir accès à toute la donnée disponible, voir figure 53.

- Étape préalable à l'analyse : intégration des données, elle permet d'avoir au sein d'un même modèle de donnée et une même interface des données issues de sources variées tel que des exports .csv et du .json, voir figure 54.

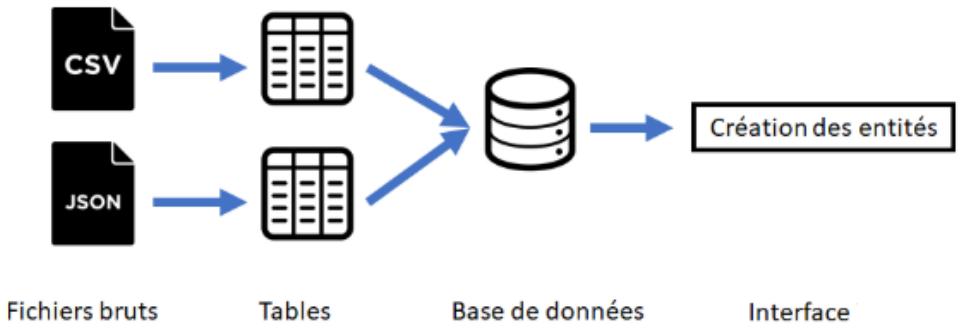


Figure 54 : Intégration des données

- Étape préalable à l'analyse : extraction d'entités et classification des documents.

  La chaîne de traitement sémantique est composée de différents types d'algorithmes supervisés et non supervisés. L'apprentissage non supervisé permet à l'analyste de découvrir les entités nommées (personnes, lieux, organisations), de classer les documents par thèmes (Singular Value Decomposition) et donc de faire un ciblage rapide dans un grand volume de documents. Par la suite, nous avons également défini des mots clés/catégories d'intérêt que nous avons extraits du texte de manière supervisée : cela nous sert à extraire des candidats, des personnages politiques et des partis déjà connus, voir figure 55.

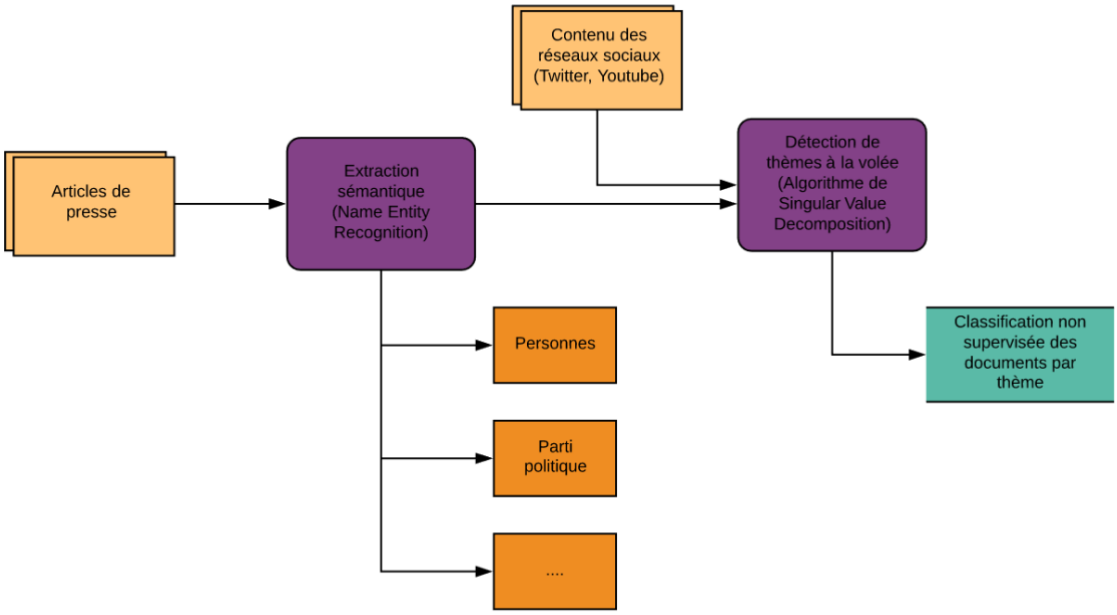


Figure 55 : Schéma d'extraction des entités

Dans la figure 56, on peut observer à gauche les différents thèmes, ici les 5 mots caractéristiques d'un sous-ensemble de texte dans un corpus. Au centre le nuage de mots représente les entités "personnes" nommées dans le corpus ; le tableau en dessous représente la liste des articles correspondant au thème sélectionné. Il est possible de prendre tous ces articles (dont on a une prévisualisation dans le panneau de gauche) et les mettre dans un environnement de travail et les explorer plus en détail.

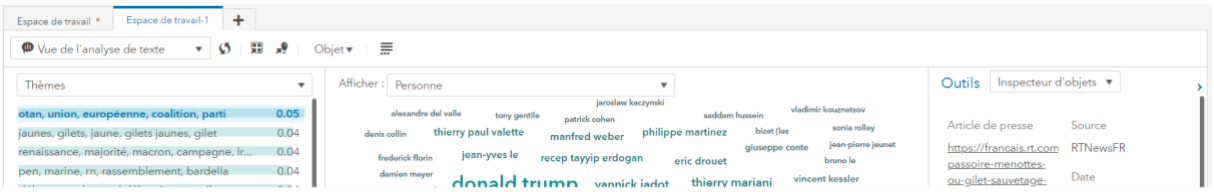


Figure 56 : Tableau de bord.

Une fois les données extraites par l'IT et intégrées par le data scientist, l'analyste est à nouveau mobilisé pour exploiter ces données via la plateforme. En développant les liens créés entre les entités, il lui est alors possible d'observer (ou non) des connexions entre plusieurs individus grâce aux mentions de personnes et de regarder attentivement quelles expressions régulières dans les professions de foi étaient reprises dans les médias et les réseaux sociaux. Il peut alors

appliquer les différents scénarios d'influence pour voir s'il y a une occurrence ou des points communs entre ce qui est analysé et les trames déjà connues. Il s'agit ensuite de rédiger un rapport de synthèse sur le procédé et les conclusions tirées à la suite de l'étude. La plateforme lui permet notamment d'identifier les similarités de champs sémantiques, les cooccurrences d'expression, les charges utiles d'influence par média et/ou cross média.

7.2.3. Cadre théorique des opérations d'influence russes

L'étude menée au mois de mai s'appuie sur un cadre théorique décrit ci-après. Chacune des méthodes connues et décrites a été recherchée au moyen d'outils d'analyse statistique, sémantique et relationnelle.

Sur la base de nos recherches académiques, nous avons pu conclure que la Russie employait trois grandes boites à « outils » dans le cadre de ses tentatives d'influence auprès des publics étrangers. Ces trois grands axes sont articulés autour des efforts suivants :

- Implication politique proactive : politique visant à tisser des liens avec différents acteurs politiques. L'objectif étant d'assister, de réorganiser et de coordonner les partis étrangers prorusses, et d'exporter ce que l'on appelle des « technologies politiques » « Pour comprendre l'impact du soft-power russe. Avec des oppositions simples : anti-américanisme vs.atlantisme ; Europe-puissance vs.Europe fédérale ; monde multipolaire vs. ce que les amis de la Russie nomment « hégémonie » américaine et plus largement anglo-saxonne ; multiculturalisme vs. identité nationale organique dans le cadre de l'Etat-Nation ».(Camus, 2018).
- La 'diplomatie de l'ONG' : créer et soutenir, par exemple, des associations orthodoxes, des groupes de jeunesses prorusses, des organisations prominorités et/ou séparatistes ainsi que des centres de réflexion choisis (Dimitrova et al., 2017).
- Création d'un environnement médiatique favorable : établir des versions en langue locale de ses organes de presse nationaux et des partenariats médiatiques (Laruelle, 2018), lancer des campagnes dans les médias russes et étrangers visant à influencer des scènes médiatiques locales ciblées en diffusant : des mensonges, des demi-vérités, et des théories du complot dans les médias […] avec un accent particulier sur l'UE et les États-Unis. (Meister, 2016).

Une fois convenus d'un cadre théorique, nous pouvions donc circonvenir un périmètre de recherche technique dans lequel il devenait intéressant d'observer les grandes thématiques employées par ces outils méthodologiques. Au regard de certaines précédentes campagnes

d'ingérence russe, nous avons réalisé que leur nouvelle politique ne semblait plus soutenir avec insistance un candidat au détriment d'un autre, mais surtout de provoquer ou d'augmenter la polarisation et de renforcer les clivages au sein des nations et des institutions transnationales, avec pour objectif de les affaiblir (Karlsen, 2019). De fait, le soutien à différents extrêmes dans le but de provoquer des dissensions est devenu la clé de voute de la politique d'influence russe sur les réseaux sociaux ou au travers de publications diverses sur le web.

Parmi les axes d'effort russe dans le numérique précédemment détectés, il est généralement admis que l'on trouve quatre grandes catégories.

- Influence directe sur les processus électoraux, support direct ou indirect aux candidats (au travers des médias sociaux, mais également en donnant plus de temps de parole à un candidat plutôt qu'à un autre au moyen de leur appareil médiatique : RT, Sputnik, etc.)
- Compromission (kompromat, contraction russe de dossier compromettant) d'un parti ou d'un candidat (publication de vidéos embarrassantes, de documents incriminants, etc.) panoplie de moyens déjà employés lors des élections américaines en 2016 ou avec les données de l'Union européenne sur l'immigration obtenues par des groupes de hackers identifiés comme russe et fournis à des partis politiques italiens prorusses avant les élections parlementaires ou bien les MacronLeaks, non-officiellement attribuées.
- Influence eurosceptique : voyant fleurir les partis anti-européens ou eurosceptiques, toujours plus vocaux l'approche des élections, il est intéressant de noter que ces derniers ont souvent une vision bien plus amicale des relations russo-européennes que la majorité de la population. Pour illustrer cette tendance, nous avons apporté un regard appuyé à tout mouvement se revendiquant d'une volonté de frexit ? (Mais également Dexit, Itaxit, etc.)
- Division de la société : dans le cadre d'un soutien à des forces centrifuges opposées visant à affaiblir les institutions étatiques et européennes, nous avons axé notre lecture des informations au prisme des sujets / catégories suivantes :
  - Gilets jaunes
  - Parties d'extrêmes
  - Immigration (crise anxiogène source de nombre de fake news de tout bord)
  - Climat (un moyen détourné de critiquer les pays arabes faisant la promotion d'énergies fossiles)

  - Crise de l'énergie
- Taxes / impôts (influence visant à créer un clivage entre riches et moins riches)
- Soutien à des causes proches des minorités en vue de les radicaliser (partis ou organisations séparatistes / indépendantistes - à l'image du référendum en Catalogne).
- Relation avec la Russie : la Russie n'hésite pas à user de relais d'influence plus traditionnels, comme sa diaspora ou les associations d'amitié fraternelle. À cet égard, il pouvait être intéressant de suivre les communautés numériques suivantes :
  - Associations de jeunesse (scout de France, d'Europe)
  - Association d'amitié franco-russe (la plus connue, parce qu'elle revient souvent dans les études sur l'ingérence russe, pour avoir des liens avec le Kremlin est "l'Association de Dialogue Franco-Russe")
  - Organisation d'outreach religieux d'origine orthodoxe, très actives, dont certaines pouvant être très proches du Kremlin

Il est à noter que pour altérer la confiance de certains citoyens européens à l'égard envers leurs concitoyens, offrir un soutien numérique (sous quelque forme qu'il soit) aux deux bords d'une même thématique devient un moyen efficace de promouvoir la méfiance. À l'image de certaines opérations médiatiques russes aux États-Unis en 2016 au Texas ayant déclenché des émeutes bien réelles suite à la création de deux groupes Facebook antagonistes bien réels sur le sujet de l'immigration et de l'extrême droite (Michel, 2017).

7.2.4. Modes opératoires

Nous avons axé nos efforts sur les actions numériques suivantes (parfois déjà répertoriées par d'autres acteurs de la communauté du renseignement ou par la presse) :

- Opérations visant à partager massivement certains hashtags pour tenter de les faire apparaître régulièrement dans les tendances de Twitter (par des bots ou des relais humains d'influence) et les voir repris par d'autres médias.
- Boucles thématiques, catégories narratives (Contenu pro-iran, pro-bashar, anti-merkel, antipolitique libérale, anti-OTAN, anti-Ukraine, anti-juif, etc.).
- Partage d'éléments de langage, avec une apparition soudaine de phrases-chocs ou de certains slogans de manière apparemment anodine ou non-coordonnée, mais toujours orientée.

- Pression et harcèlement sur des figures de mouvement.
- Faux montage (photo ou vidéo, avec une attention particulière à l'apparition de Deep-fake).
- Memes : il s'agit d'un dessin, d'une photographie, transmise par voie virale ornée d'un texte qui se moque d'un symbole culturel ou d'une idée sociale, il permet de créer l'émoi par la peur ou la dérision par le satyre.
- Mobilisation rapide d'opérateurs de désinformation autour d'événements réels afin de façonner la perception du public, et/ou de projeter un récit dans le zeitgeist qui correspondent à leur d'intérêt d'exacerber les divisions sociales.
- Mise en avant d'experts biaisés ou inconnus, mais affublés de titres factices.
- Faux recoupements croisés.
- Achat de followers, connexion à un grand nombre de comptes, effacement de messages (Détection de changement brusque) pour dans un premier temps donner plus de poids à un message, puis dans un deuxième temps brouiller les pistes.

Dans le cadre de la dé-crédibilisation des processus électoraux, nous avons étudié les rapports de terrain visibles sur les réseaux sociaux et destinés à provoquer le doute quant à la légitimité ou le sérieux du suffrage. Nous avons donc surveillé les actions physiques ont également été recherchées :

- Reconnaissance des lieux et des moyens de votes en amont des élections (Objectif possible : décrédibiliser le processus, faire naître le doute notamment en mettant en cause le manque de moyen ou la facilité avec laquelle il pourrait être possible de les truquer)
- Annonce de bourrage / disparition d'urne (visant à invalider le processus électoral)
- Annonce de tentative de dissimulation d'information (visant à jeter le doute sur l'impartialité des institutions gouvernementales en amont des élections)
- Faire naître un discours défaitiste parmi les minorités qui ne sentent pas représentées pour les pousser à croire que seule la violence leur permettrait de se faire entendre.

Les agents d'un réseau de propagande sur les médias sociaux peut-être divisé en trois types (ou tiers). Il existe trois termes bien distincts pour catégoriser les comptes entrant dans la composition d'un réseau visant à manipuler l'opinion : le Bot, l'Humain (aussi appelé 'Shill' ou encore Troll) et les comptes hybrides.

- Le Bot : Un bot est un faux compte (appelé botnet lorsque de multiples comptes sont coordonnés en réseau) sous le contrôle d'une organisation ou d'un gouvernement cherchant à influencer une communauté en ligne. Entités entièrement automatisées, généralement exécutées avec des scripts leur permettant de publier à des niveaux de volumes impossibles pour un humain. Ces bots peuvent également être programmés pour choisir des hashtags spécifiques ou d'autres signaux textuels. (Deux exemples : un bot Twitter qui doit retweeter certains hashtags et/ou phrases complètes dans des volumes tels qu'il aide à amplifier artificiellement un sujet spécifique).
- L'Humain (ou Shill /Troll) est une vraie personne qui participe activement à la formulation de discussions et d'opinions en ligne. Le Shill va promouvoir des entreprises, des gouvernements, des personnalités publiques et bien plus encore, dans un but de profit personnel, mais se livrant essentiellement à la propagande. Une des techniques souvent employées sera de rentrer dans un débat et d'en orienter la direction en provoquant la colère ou la peur, déviant le discours vers des sujets clivants.
- Le compte hybride : acteur humain utilisant un logiciel pour communiquer via plusieurs comptes en même temps de façon plus efficace. Cette tactique peut être utilisée pour éviter les algorithmes de détection de bot.

Le Bot est donc par nature entièrement automatisé et donc plus facilement détectable. Le Shill / Troll est un compte derrière lequel se tient un humain (comme ceux de l'agence russe Internet Research Agency) qui va avoir plus ou moins travaillé sur le contenu publié afin de le rendre plus cohérent et qu'il sera plus difficile de détecter hormis par une analyse narrative. Le compte hybride est un mélange des deux précédent, il pourra présenter certaines similitudes méthodologiques qui peuvent le rendre plus facilement détectable.

L'emploi de Bot ou de comptes hybride est aisément détectable, bien que leur force réside dans l'adoption de système pyramidal itératif. Ce même système qui se retrouve dans les techniques complexes de Search Engine Optimization (SEO). Les bots multiplient le contenu de basse qualité qui n'est repris que par les robots des moteurs d'indexation. Ce contenu va servir de base sémantique venant augmenter la visibilité des comptes ou le contenu posté par des Trolls. Cette technique a pour avantage de venir ajouter un poids sémantique autour de thématiques connexes en provenance de sites sérieux, mais dont le sujet s'inscrit dans une trame narrative orientée, ou alors d'appuyer des publications en provenance de Sputnik ou RT. Ces techniques vont donner un soutien contextuel à des entités rarement lues par des êtres humains, mais prises en compte par les algorithmes de référencement de contenu. Ces dernières sont de plus en plus

utilisées pour amplifier le contenu endogène. Plutôt que de chercher à créer du contenu efficace, on augmente la portée du contenu par des procédés statistiques qui s'appuient sur la génération de contenu polarisant qui sera ensuite exploité ou produit par les forces centrifuges locales (partis extrêmes locaux, par exemple).

Afin d'inscrire notre étude à la croisée des techniques numériques les plus récentes dans le cadre des tentatives possibles d'ingérence, nous nous sommes aidés d'un corpus analytique riche dans ce domaine. Qu'ils soient d'ordre méthodologique, sémantique ou statistique, nous nous sommes astreints à compulser une somme conséquente d'analyses provenant de sources reconnues et européennes dans les domaines suivants : étude d'une base de données de fake news pour déterminer le contenu de désinformation (comme https://euvsdisinfo.eu/)Comparaison de contenu entre les bases de fact-checking et les bots/trolls connus.

A partir des éléments recueillis, de notre expérience, de notre propre étude et des outils à notre disposition, nous avons basé notre méthodologie d'automatisation comparative sur la base des critères suivants :

- Comparaison de valeurs statistiques
  - Date de création de compte
  - Ratio de tweets / par jours | Ratio trop élevé de tweets / heure. (Plusieurs analyses mettent la barre à 72 tweets par jours sur plusieurs mois)
  - Acquisition rapide d'ami / followers
  - Rapidité de post avec faible ratio de followers
  - Évaluation de la popularité (retweet/like) en comparaison du profil de compte
  - Provenance des followers
  - Comparaison des bios de comptes
  - Test du retweet (si les retweets du compte ont très peu d'engagements)
  - Rapidité de re-tweet d'une info (par rapport à sa publication)
  - Options de Geotagging
  - Absence de toute de localisation précise (ou ayant des localisations en dehors de l'Union européenne)

  - Étude des plages horaires de publication des tweet/posts par burst : Un compte qui ne publie jamais rien pendant deux semaines, mais qui se réveille dès qu'il y a une élection ou un grand événement
  - Inconsistances horaires des tweets (Création de/des profils horaires et comparaison géographique des horaires de travail à l'étranger)
  - Similitude d'horaire et de volume d'émission
- Comparaisons d'utilisation :
  - Détection des comptes multilingues
  - Détection des comptes de revendiquant une appartenance à une minorité
  - Utilisation fréquente de Headlines sans lien vers la source originale
  - Emploi d'outil d'Url Shortener (permettant de comptabiliser le trafic : grâce à ces outils, il est possible de comptabiliser le nombre exact de personnes cliquant sur le lien)
  - Retweets (quasi)exclusifs de sites orientés prorusses (Sputnik ou RT) ou de site identifié comme postant des informations orientées
  - Absence de photo de profil
  - Détection des comptes gérés par une application tierce
  - Détection de marionnettes : plusieurs personnes animent un compte
  - Détection des marionnettistes : une personne anime plusieurs comptes
  - Recherche de thématique commune via logique floue (paraphrase)
- Analyse sémantique :
  - Détection des comptes ou des auteurs qui font dévier un récit le long d'une trame narrative provoquant la haine et le ressentiment
  - Détection des comptes s'attaquant constamment à quelque chose qui ne faisait pas partie de la conversation initiale (Argumentation employant des termes tels que "mais qu'en est-il quand X a fait Y » visant à discréditer un opposant par l'emploi d'une comparaison hors contexte)
  - Analyse orthographique et grammaticale, par exemple : l'absence partielle de 'un/une' ou de 'le/la' peut être un marquant dans un post (en russe, la détermination

genrée n'existe pas et que les auteurs russes oublient de l'ajouter quand ils rédigent en français)

- Utilisation de technique morphosyntaxique de clickbait / piège à clic

7.2.5. Résultats et comment les améliorer

Dans notre recherche d'influence, d'après ce que nous avons pu surveiller sur le mois de mai 2019, il n'y a pas eu d'influence étrangère sur les élections européennes en France. Rien de significatif n'a été observé dans les médias utilisés pendant ce type d'événement (presse écrite/numérique et médias sociaux). Ce constat d'absence d'influence pourrait donc s'expliquer de plusieurs façons, la première d'entre elles étant la non-exhaustivité de notre collecte de données. Une autre explication possible, en pleine période de Brexit, la France n'a peut-être pas été une cible parce que le pays était suffisamment déstabilisé par les gilets jaunes ou parce que les têtes de liste n'avait aucune notoriété préélectorale limitant de fait leur impact. Cette étude démontre notamment la nécessité d'une permanence de la recherche et détection d'opération d'influence étrangère sur les intérêts de la France. En se basant sur des scénarios connus des méthodes d'influence, il ne semble pas qu'ils aient été repris durant la campagne 2019. On ne détecte pas de mouvance majeure : les messages similaires les plus fréquents appelaient à aller voter. Dans nos analyses, nous avons surtout remarqué que les appels à aller voter étaient internes avec notamment les gilets jaunes qui appelaient à voter « contre » le président de la République (et donc la liste Renaissance) et non pas « pour » une liste en particulier. La représentation des gilets jaunes dans diverses listes lors des élections européennes a condamné tout appel au vote massif pour un parti spécifique.

Tant la robustesse de notre méthodologie DETEVEN que la nature de l'objectif de l'adversaire nous auraient permis à coup sûr de détecter toute forme d'opération influence si elle était encore en cours quand nous avons commencé notre observation. Chaque suivi en temps réel ou analyse a posteriori permet d'améliorer le modèle de DETEVEN pour permettre à termes de le déployer en permanence comme outil de défense de l'opinion publique.

7.3. Application sur une analyse de fake news

7.3.1. Méthodologie

Le suivi automatique de fake news peut se faire de deux façons : soit le contenu sémantique se distingue très nettement de la charge sémantique des autres vecteurs d'information portant sur le même sujet, soit la viralité du vecteur est artificiellement augmenté. Ce dernier point se détecte facilement par le suivi de diffusion d'url par exemple. Lorsqu'un fake news est détecté, une plateforme doit être utilisée pour en identifier les origines et la cible. Cette analyse est effectuée Top-Down, en partant d'une granularité fine comme un candidat, un parti, un message, puis en identifiant les vecteurs et les messages d'expression de soutiens pour remonter jusqu'à une entité plus large).

7.3.2. Contexte

La guerre civile en Syrie, en cours depuis 2011, a morcelé le pays en plusieurs secteurs d'influence et de contrôle distincts. Les forces fidèles au gouvernement contrôlant à ce jour la majorité du territoire, il ne reste aux mains de l'Armée Syrienne Libre (ASL) que les régions d'Idlib, au nord, et de Al-Tanf, au sud. Les autres régions étant sous le contrôle d'autres entités soutenues par des puissances étrangères, le régime syrien n'est pas en mesure d'y lancer des campagnes de reconquête. Depuis 2013, les régions contrôlées par les rebelles ont vu arriver diverses organisations humanitaires de protection civile, comme l'Organisation de la Défense Civile Syrienne (ODCS), dont les membres sont aussi appelés les "Casques Blancs". Les Casques Blancs ont commencé leurs opérations en tant qu'organisation indépendante composée de bénévoles, mais elle est aujourd'hui financée par plusieurs gouvernements étrangers, notamment les États-Unis, la France, le Royaume-Uni, les Pays-Bas et le Japon, ainsi que par des donateurs privés. L'organisation affirme disposer d'un budget de 26 millions de dollars (2018) et s'identifie comme neutre face au conflit, sa principale mission étant de sauver des vies, dans les deux camps. Bien que professant sa neutralité, elle n'en demeure pas moins contrainte à opérer dans les zones contrôlées par les rebelles, car elle est le centre d'une attention particulière de la part du régime syrien, qui lui refuse catégoriquement l'entrée dans les zones qu'elle contrôle. Ces « Casques blancs » sont devenus la cible de nombreuses attaques tout en étant régulièrement accusés d'avoir un rôle bien plus actif dans ce conflit armé que l'ODCS ne

l'admet. En effet, des théoriciens « conspirationnistes » les ont assimilés aux djihadistes qui s'activent à attirer les Occidentaux dans un conflit ouvert avec la Syrie. Les propos sont alors nombreux pour tenter de décrédibiliser les actions de ces bénévoles. Pour les puissances occidentales, une quelconque intervention en Syrie ne saurait être justifiée sans véritable raison. L'utilisation d'une arme chimique en est une, cette dernière étant proscrite par les Conventions de Genève. C'est pourquoi en 2013, les États-Unis, soutenus par la France et la Grande-Bretagne, avaient hésité à intervenir en Syrie avant d'y être contraints par le massacre de la Ghouta (21 août 2013). C'est également sur cette même logique que ces trois pays se sont mobilisés suite à l'Attaque chimique de Khan Cheikhoun (4 avril 2017). Dans son incessante bataille pour les esprits, les organes de propagande russe n'ont alors eu de cesse de discréditer les Casques Blancs en publiant ou relayant de fausses informations.

Dans le cadre de cette étude, nous avons délimité notre périmètre de recherche aux réseaux sociaux (Twitter et Facebook) et quelques blogs en français et en anglais afin d'observer toute tentative d'influence ou de manipulation des médias en faveur du relai de la fake news étudiée. Nous avons appliqué notre méthodologie sur des médias traditionnels (presse écrite, numérique) et sur les réseaux sociaux (notamment Twitter). Les politiciens, les journalistes sont présents sur différents médias et visent à toucher un plus grand nombre de lecteurs en diffusant sur plusieurs plateformes à la fois. À ce titre, les acteurs de ce relai utilisent donc une multitude de médias pour impacter un maximum de personnes en fonction des tranches d'âge et des catégories socioprofessionnelles visées (télévision, journaux, sites d'information, réseaux sociaux dont Facebook, Twitter, Instagram et YouTube). Nous avons donc décidé de porter nos recherches sur plusieurs médias pour accroître nos chances de détecter une tentative de diffusion de masse de fake news. En revanche, notre accès restreint aux données de Facebook nous a contraints à surtout nous baser essentiellement sur Twitter comme réseau social pour la collecte du fait d'absence de contenu significatif sur les autres médias numériques (Instagram, YouTube).

7.3.3. Les faits

Selon des informations en date du 29 mars 2019 et provenant d'un général russe, Viktor Kouptchichine, les services de renseignement français et belges auraient préparé une ou des attaques chimiques dans la province syrienne d'Idlib, en coordination avec des cellules terroristes évoluant dans la localité ainsi que des Casques Blancs (White Helmets). Les services de renseignement auraient eu l'intention de filmer une mise en scène macabre, d'en trafiquer

les images et de s'en servir comme autant de preuves de la participation active de Moscou à l'attaque. Cette information fait ainsi suite à des mises en garde répétées de la part de la Russie quant à des opérations occidentales « sous faux pavillon » (false flag) en Syrie. À cet effet, elle a déjà prévenu l'opinion publique de probables attaques chimiques en 2013 et en 2018. Ces allégations auraient ensuite servi de justification à des frappes aériennes de la coalition contre les troupes du gouvernement syrien (notamment en 2017 lors de l'attaque de Khan Cheikhoun). Cette information a été démentie par le ministère français des Affaires étrangères et par le ministre de la Défense belge, qui a donné l'assurance de son strict respect de la Convention de Genève sur les armes chimiques.

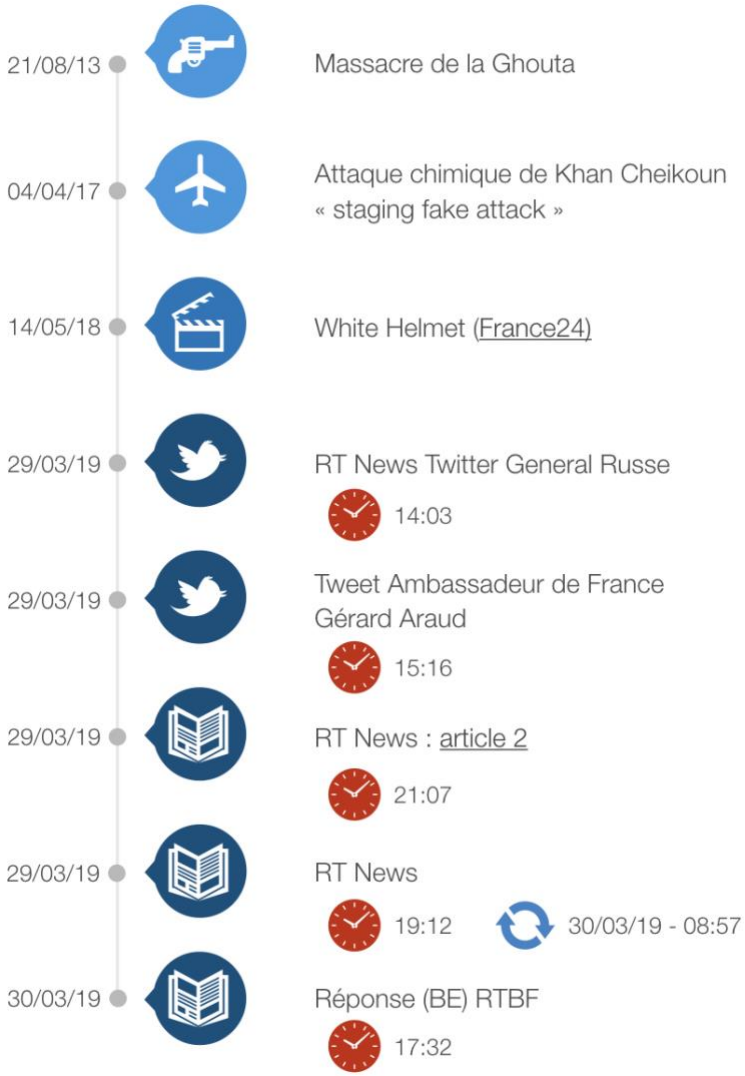


Figure 57 : Chronologie de la fake news (France24, 2018 ; RTBF, 2019)

7.2.4. L'origine de la fake news

La fake news portant sur l'implication occidentale dans de potentielles attaques chimiques sur la Syrie n'est pas une nouveauté. Lors de l'attaque du 21 août 2013, de nombreuses personnes ont analysé les événements et ont conclu à un coup monté de la part des forces occidentales pour donner une "raison" d'intervenir et d'enquêter sur le sol syrien. La principale « preuve » mise en avant à ce moment était notamment la date de publication de certaines vidéos mises en ligne... la veille de l'attaque. Pour appuyer ses propos concernant les faits inventés de toute part par l'Occident, le réseau Voltaire trouve même des similitudes entre les images soi-disant prises en Syrie et des images utilisées pour accuser l'Armée égyptienne d'avoir massacré un campement des Frères musulmans au Caire. Tout cela, non sans mentionner également les mensonges de Colin Powell, secrétaire d'État américain qui avait avoué que les preuves détenues pour accuser l'Irak de posséder des gaz de combat étaient fausses, moyen de proposer une comparaison avec les faits relatés en 2013 concernant la Syrie et l'attaque chimique (Réseau Voltaire, 2013).

Figure 58 : Extrait de l'article en ligne "Gaz sarin en Syrie : nouvelle opération de propagande", (Réseau Voltaire, 22 août 2013)

Pour la récidive du 4 avril 2017, le blog de Stéphane Montabert affirme que le responsable de l'attaque Khan Cheikoun aurait visé un "dépôt rebelle contenant des armes chimiques". Pour lui, il est incohérent qu'Assad ait ciblé de manière non conventionnelle un lieu détenu des ennemis du régime dans un contexte géopolitique en sa faveur (Donald Trump venait d'affirmer

que la victoire contre l'État Islamique était prioritaire sur l'éviction du président syrien). Pour le libéral suisse, l'intervention quasi immédiate des États-Unis qui suivait l'attaque de Khan Cheikoun appuie davantage cette interprétation des faits comme étant montés de toute pièce (Montabert, 2017).

La fake news du 29 mars 2019 que nous avons étudié part de la déclaration du général russe Viktor Kouptchichine. Pour celui-ci, les services secrets français et belges participeraient à l'organisation d'une provocation à l'arme chimique en Syrie pour piéger Moscou et Damas (Russia Today, 2019). L'information relayée par le site RT France puis poussée par Sputnik (Sputnik News, 2019) tente de prouver qu'il y a un lien entre cette tentative d'attaque chimique et le fait que la Maison-Blanche s'était proposée quelques jours avant (le 17 mars) de mettre 5 millions de dollars (environ 4,4 millions d'euros) à la disposition des Casques blancs et du mécanisme de l'ONU chargé de faciliter les enquêtes sur les violations du droit international en Syrie.

Le député Nicolas DHUICQ (Les Républicains) est d'ailleurs le premier à avoir repris l'information sur Twitter. Connu pour ses propos virulents sur différents sujets (homosexualité, politique, migration…), il ne cache pas une certaine sympathie envers la politique de Vladimir Poutine et la Russie. Russophone, le maire de Brienne le Château n'a mis que quelques heures à peine pour informer ses abonnés de toute cette affaire décrite par Sputnik News.

Figure 59 : Tweet de Nicolas DHUICQ du 29 mars 2019

7.3.4. Les moyens de relayer de la fake news

Dans le périmètre de cette étude, nous avons abordé trois relais de viralité pour mesurer l'impact de cette information. Deux médias sociaux, Twitter et Facebook (bien que ce dernier ait été moins exploité par notre analyse), ainsi qu'un survol de la blogosphère prorusse. Nous pouvons rapidement constater que l'information suivie a eu un faible impact, et ce, dans un intervalle temps très limité. On trouve néanmoins certaines publications qui méritent plus que d'autres d'être mentionnées. Par exemple, le tweet de Nicolas Dhuicq contenant le lien d'une vidéo russe non répertoriée intitulée "Saisies de cachettes d'insurgés".

Figure 60 : Tweet de Nicolas DHUICQ du 17 avril 2018

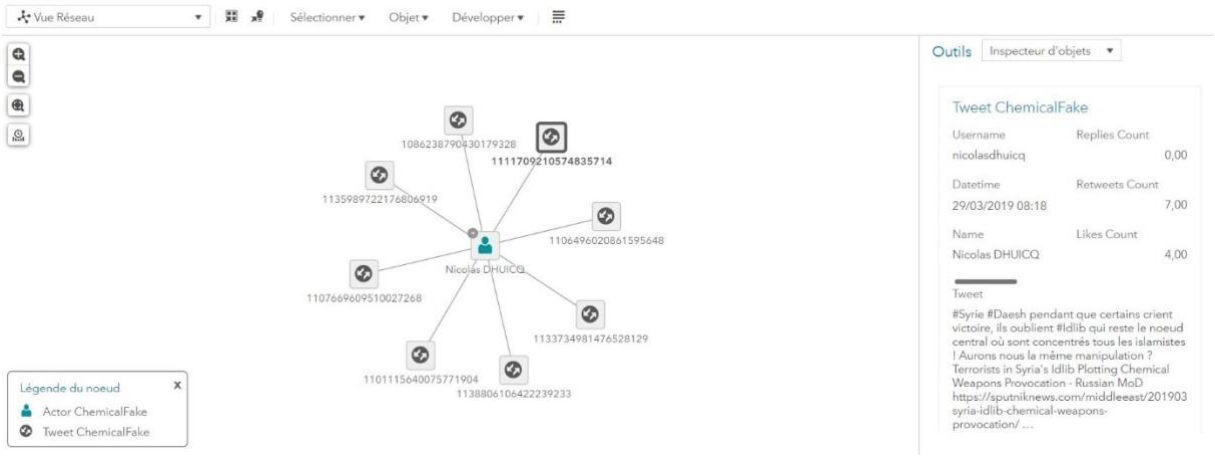


Figure 61 : Extrait de notre plateforme présentant tous les tweets de Nicolas DHUICQ

Figure 62 : Extrait de notre plateforme présentant les expressions à 3 termes récurrentes

Le billet du réseau Voltaire concernant l'attaque chimique du 21 août 2013 présente même un bon nombre d'outils qui permettent de mettre en lumière ce qui lui semble être une action mise en scène par les Occidentaux (photos reprises lors de diverses informations, défaut de chronologie des faits...). De même, ce billet n'a été que peu partagé sur les réseaux et les commentaires sont relativement peu nombreux à accorder de la crédibilité aux faits relatés.

7.3.5. L'impact de la fake news

Le peu d'écho que l'information originelle (2019) a provoqué dans la twittosphère est à mettre en rapport avec le peu de visibilité dont ladite information a bénéficié sur la galaxie de blogs prorusses de renom ou proches de mouvances extrémistes diverses, en dehors des blogs poubelles.

- Twitter

La particularité du partage d'URLs sur twitter repose sur un système interne de « raccourcissement » de liens (url shortening). La fake news peut de fait être partagée par plusieurs comptes Twitter, mais pas par la même URL. Ce qui rend d'autant plus difficile la cartographie sociale de partage et de diffusion de l'information.

Après une période de collecte de données sur Twitter en français et en anglais entre le 25 mai 2019 et le 10 juin 2019, dont l'intégralité des tweets de Nicolas DHUICQ, on constate que l'information n'a pas bénéficié d'un relai de croissance exponentielle comme d'autres campagnes de propagande colportées sur ce média. De même, le faible engagement des comptes habituellement prorusses (en dehors de celui de l'ancien député Nicolas DHUICQ) n'a probablement par permis à l'information d'être disséminée de manière optimale.

À l'inverse, les tentatives de démenties de l'information suivie ont bénéficié d'une viralité plus importante que l'information elle-même (voir figure 63 : tweet de Gérard Araud, ancien ambassadeur français). Le résultat est que ce fake new, bien que peu remarquée, a néanmoins provoqué une forte riposte.

Figure 63 : Tweet de Gérard Araud du 29 mars 2019

- Facebook

Confrontés aux difficultés inhérentes posées par l'analyse des comptes Facebook, pour la plupart fermés, et par les pages aux accès réservés, nous n'avons pas été en mesure de procéder à une analyse poussée de la diffusion de cette fake news dans la communauté francophone dudit réseau social. Nous pouvons néanmoins procéder à une constatation statistique de sa viralité. Il apparait, aux vues des indicateurs auquel nous avons eu accès, que l'information n'a pas gagné de traction particulière auprès du publique visé. Les sujets ayant traits à la Syrie et postés sur le compte Facebook de RT dépassent rarement les 200 commentaires et les 300 partages. L'information suivie rentre donc dans la moyenne basse de la viralité habituelle pour ce genre d'information.

- Blog / Sites internet

À la différence des réseaux sociaux susmentionnés, l'information suivie (en lien direct depuis des URLs pointant vers RT / Sputnik ou bien partageant un espace sémantique de sens commun) apparait plus massivement dans la blogosphère peu après les déclarations du général Viktor Kouptchichine. Ces blogs participent activement à la soupe consonantique prorusse, un levier d'influences sur les moteurs de référencement web et un relai de croissance virale que d'aucuns appelleraient des "blogs poubelles" (Junk blogs). Il est à noter que l'annonce du général Kouptchichine ne fait généralement pas l'objet d'un suivi rédactionnel dans la durée. Ce qui tendrait à démontrer que les démenties étayés ont pu rapidement participer à stopper la propagation de cette fake news. Il est néanmoins virtuellement impossible de juger de l'impact de la diffusion d'informations, quelles qu'elles soient, au travers de cette galaxie de blogs et de sites internet secondaires. En effet, nous avons remarqué que la plupart des plateformes de commentaires sur ces sites internet se faisaient généralement hors de l'espace de Twitter, mais plutôt sur Facebook et Disqus (ce dernier est une plateforme de commentaires multisites très prisée par les sites alt.right américains). Nota bene : au même titre que pour Twitter, suivre la dissémination d'une fake news par une URL se heurte à la même problématique des services d'URL shortener comme t.co, bitly, goo.gl, etc. N'étant pas en mesure de reverse-engineering l'ensemble des URL raccourcis pour une URL de départ (RT ou Sputnik), traquer l'émergence et le partage de l'information ne peut devenir que parcellaire.

7.3.6. Notre analyse

Les campagnes de fake news en provenance des agences d'influence russes (Troll Farms) fonctionnent souvent de manière empirique. Elles génèrent tout d'abord un bruit de fond permanent composé de fausses informations, abordées plus ou moins sérieusement, en attendant de voir celles qui provoqueront l'écho émotionnel le plus fort auprès des publics ciblés.

Dans un souci de rationalisation des moyens cyber et afin d'obtenir les effets les plus percutants, il devient alors logique de ne sélectionner que les fake news qui semblent plaire et provoquer le bruit médiatique le plus impactant et clivant. Ces dernières peuvent ensuite bénéficier d'un suivi plus personnalisé (soutien par des réseaux de bots, comptes hybrides, comptes identifiés appartenant à des figures politiques ou médiatiques installées, relai dans la presse traditionnelle, témoignage, etc.). Au prisme de cette interprétation, il est cohérent de constater que ce n'est pas la première, mais la troisième fois, que cette fake news spécifique est relayée dans les médias. Une première fois en 2013, une seconde en 2018 et aujourd'hui en 2019. Le souci de recyclage des fake news à intervalle régulier est emblématique de ce qui semble caractériser les campagnes de fausses informations russes et cette dernière n'échappe pas à la règle. Concernant la nature même de l'information, il est intéressant de noter que le Ministère russe de la Défense ne fournit aucune preuve venant appuyer les affirmations du général Kouptchichine. Les seuls éléments abordés sont d'ordre "scénaristique" :

- Le moment choisi pour l'opération.
- Les parties en présence (Services de renseignement français et belge, casques blancs, Hayat Tahrir al-Cham et Tanzim Hurras ad-Din).
- Des informations parcellaires portant sur les substances chimiques devant être utilisées.
- Des éléments temporels soi-disant incohérents.
- Des éléments géopolitiques allant dans le sens d'une mise en scène.

Une information connexe, en date du 11 septembre 2018 et publiée par RT (Russia Today, op. cit.) se fait déjà l'écho de la participation de Casques Blancs à des mises en scène présumées d'attaques chimiques dans la région de Jisr-al-Choghour. Les Casques Blancs apportant une aide humanitaire après ce que RT appelle "une attaque de bombes-barils prétendument menée par des avions de l'armée syrienne". L'information de 2019 publiée par RT fait donc partie d'un ensemble narratif clairement en faveur du régime syrien tout en accusant les gouvernements et les organisations occidentales d'être "responsables d'attaques sous faux pavillon" en Syrie (Russia Today, 2019). Au travers de cette information, RT décrit les casques blancs comme des

terroristes soutenus par des puissances occidentales ennemies pratiquant l'ingérence à outrance. Ces actions pourraient alors avoir comme objectif de pousser l'Occident à mener des enquêtes en Syrie, voire y envoyer des troupes en raison de la transgression aux Convention de Genève qui en résulterait. À tout le moins, elle provoque une désensibilisation de l'opinion publique occidentale qui, finissant par se lasser, en viendrait probablement à ne plus s'offusquer de quelconques exactions commises dans la région, tout en désirant encore moins chercher à en connaître ses auteurs réels. Au même titre qu'en 2018, aucune preuve n'a encore été apportée par la Russie prouvant que les Casques blancs se seraient associés à des services de renseignement occidentaux ou à des groupuscules armés visant à mener des frappes chimiques ou auraient participé à la mise en scène d'une attaque pilotée depuis l'étranger En dépit des "avertissements" répétés de Moscou sur des attaques chimiques imminentes (réelles ou planifiées) mises en œuvre par des puissances occidentales, les preuves disponibles continuent obstinément à pointer du doigt le régime syrien. En septembre 2018, les enquêteurs des droits de l'Homme des Nations Unies avaient identifié 39 attaques chimiques perpétrées en Syrie entre 2013 et 2018, dont 33 attribuées à Damas. Les auteurs des six autres doivent encore être identifiés.

La mention de la France et de la Belgique n'est pas non plus une occurrence rare dans la rhétorique russe. La France est souvent victime d'offensives numériques de la part de la Russie. Quant à la Belgique, déjà en 2016, elle avait dû faire face à des accusations du Kremlin qui déclarait alors que des avions de combat belges avaient tiré sur un village situé à proximité de la ville d'Alep (Russia Today, 2016). Les autorités belges avaient alors démenti cette information en précisant qu'aucun avion de l'armée de l'air belge n'était présent dans la région d'Alep au moment de l'incident. Concernant l'étude de l'impact et des effets recherchés, il est évident qu'au vu du manque de relai et de l'absence de viralité sur les réseaux sociaux, cette fake news n'a pas trouvé suffisamment de résonnance dans la communauté internet prorusse pour susciter un quelconque engouement.

Le manque de suivi, de partage ou d'expression de sentiment (au travers des commentaires) laisse à penser que l'information, bien que régulièrement recyclée, peine à trouver un auditoire qui lui serait suffisamment sensible et qui pourrait justifier un traitement plus poussé (usage de bots, etc.) La topologie et le suivi des "blogs poubelles" sont quant à eux liés à des techniques éprouvées de sites pyramidaux utilisés dans la manipulation des techniques de Search Engine Optimisation. Ces derniers visent à créer un contenu rédactionnel de piètre qualité destiné à apporter un contexte sémantique devant manipuler les algorithmes de référencement des

moteurs de recherche. Ainsi, cela permet à un jeu d'informations de remonter en priorité dans les flux personnalisés d'informations d'usagers réels de ces plateformes.

Finalement, bien que l'information suivie n'ait, semble-t-il, pas eu d'impact significatif sur internet ou dans les médias traditionnels (hormis à provoquer la publication de démentis en cascade), le matraquage incessant des esprits, même de manière périphérique, finit souvent par créer un nuage émotionnel qui s'affranchit des réalités et du fact-checking.

7.4. Conclusion

La recherche d'influence est une activité nécessaire et permanente. Seule une méthodologie éprouvée et explicable telle que celle décrite dans ce chapitre permet d'affirmer qu'aucune opération d'influence n'a eu lieu sur les réseaux sociaux lors des élections européennes en France en 2019. Une méthodologie ne suffit pas pour autant, il faut également des systèmes de collecte et de traitement ainsi que des analystes formés à ce métier de veille stratégique. L'insertion de la fake news étudiée a été un échec en Occident, mais le recyclage et l'enrichissement de celle-ci au fil des ans tend à démontrer l'insistance des agents d'influence usant des médias et des relais viraux russophones. La question vient à se poser : la répétition de cette méthode va-t-elle porter ses fruits ou va-t-elle continuer d'avoir un faible impact sur l'opinion publique ? Si une quatrième tentative de relai d'une fake news mettait en avant l'implication française ou occidentale dans une attaque chimique en Syrie, aurait-elle davantage l'effet escompté ? Ou serait-elle à nouveau relayée par quelques proRusses sur twitter entre deux tweets sur une élection ou un fait divers ?

Il est intéressant à noter que cette information, qui vient s'ajouter à d'autres du même ordre, précède de moins de trois semaines une nouvelle campagne militaire du régime syrien pour reprendre Idlib, même si ce parallèle est extrêmement hasardeux à dessiner au vu de la constance des Troll Farms russes et de la permanence de leurs attaques. Pour améliorer nos résultats, il faudrait reprendre la méthodologie Bottom-Up décrite dans la première partie avec un plus large spectre de collecte pour une analyse post événement. Cela nécessite un achat de donnée amont et une collecte en temps réel fourni par le média (par exemple ne pas se limiter à quelques hashtags, mais prendre tout ce qui concerne une certaine zone géographique). Ensuite, il faudra réaliser des études sur les autres médias et observer les coordinations si elles ont lieu. Il faudrait également reprendre la méthodologie Top-Down : veille permanente avec un suivi ciblé sur certains vecteurs qui permettrait de constituer des dossiers de fond préparatoires à l'analyse : sites connus d'influence étrangère, des commentaires YouTube, des sites de dénonciation de fake news, comptes twitter, ...

Cette approche permettrait par exemple de mettre en veille des influenceurs acquis à l'adversaire, des botnets, voire des charges sémantiques, et de générer des alertes sur leur réapparition. Ceci permettrait de générer des alertes sur une mouvance, sur la préparation d'un événement, avec de la détection de fake news, détection de viralité artificielle. Il serait alors possible d'effectuer un suivi de thématiques, il est également possible de faire du geofencing

(c'est-à-dire de la sélection géographique de données) à l'échelle départementale (comme les différents « départements en colère, genèse des gilets jaunes) voire européenne. On suit un sujet déjà géolocalisé qui se déplace sur une autre zone (même #, même phrasé, exemple : mouvement anti-compteurs Linky). Le volume est détecté, l'impact mesuré, l'ampleur potentielle du mouvement qualifiée, déplacement des contestataires d'une zone à l'autre détecté. Enfin, l'emploi des méthodes avancées de Traitement Automatique des Langues pour faire de la détection d'auteurs. Le pool de Trolls spécialisés est réduit, les avancées techniques en NLP, une fois adaptées à des besoins spécifiques, permettent dorénavant de répertorier certaines caractéristiques d'écriture et de les attribuer à un ou plusieurs auteurs. Sur le temps long, grâce à des algorithmes de machine learning, on serait alors en mesure de surveiller les thèmes cibles et l'analyste pourrait être alerté lorsque ce thème serait surreprésenté.

L'influence électorale et la fake news sont deux armes du soft power sur lesquels n'existent aucune réglementation internationale, aucun adversaire dans un conflit n'a de raison s'en priver, encore moins dans un conflit permanent telle qu'une guerre hybride. Ces armes impactent un moyen de pression sur un gouvernement en place, endémique dans toute société : le mouvement social. En contrepartie, elles appellent à la mise en œuvre de nouveaux processus de renseignement et de plateformes associées tels que nous les décrivons dans nos travaux. Même si aujourd'hui les liens entre mouvement social numérique et mouvement social physique ne sont pas clairement expliqué, une forme d'influence existe, elle n'est pas encore maîtrisée, ni par le monde académique ni par le monde du renseignement.

Lorsqu'une plateforme telle que Facebook change son algorithme de suggestion de contenu, selon les mots de son fondateur Mark Zukerberg : « *Je suis en train de changer l'objectif que je donne à nos équipes de produits, qu'ils ne se concentrent plus à vous aider à trouver du contenu pertinent, mais à vous aider à avoir des interactions sociales plus significatives.* », cela se traduit par : « *Pour ce faire, nous allons prédire les messages sur lesquels vous souhaitez interagir avec vos amis, et afficher ces messages plus haut dans le flux. Il s'agit de messages qui inspirent des discussions en va-et-vient dans les commentaires et les messages que vous voudrez peut-être partager et auxquels vous voudrez peut-être réagir - qu'il s'agisse d'un message d'un ami demandant conseil, d'un ami demandant des recommandations pour un voyage ou d'un article ou d'une vidéo qui suscite beaucoup de discussions.* » pour les développeurs. (Facebook, 2018).

Il paraît clair que des messages polarisants, clivants, du type de ceux susceptibles de provoquer une influence, ou une fake news, correspondent en tout point aux règles de promotion de

contenu de cette plateforme. La recherche académique en sciences humaines et sociales en particulier les axes portant sur les politiques du conflit, l'influence sociale, la mobilisation et les sciences de l'information et de la communication peuvent contribuer à la détection de nouvelles méthodes d'influence étrangère au moyen des plateformes les plus impactantes, les plus imbriquées dans notre quotidien.

8. Chapitre 8 : La police guidée par le renseignement

8.1. Introduction

> *Ce que l'on conçoit bien s'énonce clairement, Et les mots pour le dire arrivent aisément. (Boileau, 1674).*

Il serait illusoire d'affirmer que le concept de police prédictive corresponde à l'énoncé de Boileau. Depuis son apparition dans les années 90, elle croule sous le nombre de définitions, de supporters et de détracteurs. La police n'échappe pas à la montée en puissance du big data, qu'il s'agisse des données qu'elle génère ou des données auxquelles elle a accès, on attend d'elle qu'elle soit en mesure de mieux les exploiter, que l'exploitation de ces données améliore son efficacité et son efficience comme pour toute entreprise. Cette exigence est légitime. Cependant la police n'est pas une entreprise ni un service de renseignement militaire. Elle agit dans un cadre légal particulier au profit d'un gouvernement, d'une société, sur des concitoyens qui disposent d'autres droits qu'un client ou qu'un ennemi. Face à ces grandes attentes en termes de performance, la police, américaine en particulier, a fait la promotion d'un modèle surprenant : la police prédictive. L'exploitation des données au moyen de logiciel, et d'intelligence artificielle, permettrait tout simplement de prédire les crimes. Dans la première partie de ce chapitre, nous comparerons la police prédictive aux autres modèles de police, expliquerons ce qui est réellement sous-entendu par ce concept et en quoi le modèle de police guidée par le renseignement s'en distingue. Dans un second temps, nous nous baserons sur les éléments recueillis dans les appels d'offres des deux dernières années et des entretiens avec des policiers pour définir les bases d'une plateforme de renseignement policier. Enfin, pour s'affranchir du concept de police prédictive nous en étudierons les limites en particulier celle du profilage et conclurons sur les attentes de la police guidée par le renseignement.

8.2. La police prédictive et/ou la police guidée par le renseignement

Dans la littérature dédiée, essentiellement anglo-saxonne, l'amélioration des performances des forces de l'ordre est souvent nommée indifféremment *predictive policing* (police prédictive) ou *intelligence-led policing* (police guidée par le renseignement). L'exploitation logicielle des données policières des partenariats entre des polices municipales et des universités américaines et les plans de renseignement policier mis en œuvre au Royaume-Uni au milieu des années 90. Le postulat de base part du constat que la police perd trop de temps à répondre à des situations d'urgence et qu'elle doit reprendre l'initiative en visant (targeting) préventivement les délinquants connus (profiling). Cette exploitation logicielle des données s'est étendue en Australie et en Nouvelle-Zélande, avant de connaître un nouveau succès aux États-Unis après les attentats du 11 septembre 2001. La police prédictive est l'objet de nombreux fantasmes, d'aucuns la comparent au film *Minority Report* dont le sujet est l'arrestation préventive (et la condamnation) de criminels avant qu'ils ne commettent leurs actes. Ces attentes ont été renforcées par les sirènes des services marketing des vendeurs de logiciels. Cette approche a pour objectifs de permettre de réagir aux tendances plutôt qu'aux événements, et de prévenir plutôt que détecter en étant proactif plutôt que réactif au travers d'opérations planifiées plutôt qu'imprévues. Ce modèle se distingue de différents modèles mis en place au travers de l'histoire listés par Jerry Ratcliff (2008) et repris par l'Organisation pour la sécurité et la coopération en Europe :

- *Le maintien de l'ordre traditionnel fait référence à un style réactif et axé sur les incidents dans lequel les officiers de police répondent aux crimes et aux demandes d'intervention. Répondre aux appels, recevoir des plaintes, patrouiller au hasard pour afficher une présence visible de la police et pour enquêter sur des crimes qui se sont produits ou se produisent sont l'essence même du maintien de l'ordre traditionnel.*
- *La police de proximité met l'accent sur le partenariat entre la police et la communauté pour répondre de manière proactive aux préoccupations en matière de sécurité et de sûreté. Le maintien de l'ordre axé sur la communauté vise à instaurer la confiance et à accroître la communication entre la police et le public. Les programmes de police communautaires incluent la création de forums communautaires avec la participation de représentants de divers groupes communautaires et institutions où les*

préoccupations en matière de sécurité, y compris les incidents liés à la criminalité locale et les faits nouveaux, sont abordés, discutés et adressés.

- *Dans la police axée sur les problèmes, l'identification et l'analyse du « problème » constituent la base le travail de la police, plutôt qu'un crime, une affaire, un appel ou un incident. Le modèle met l'accent sur le problème à l'origine de la criminalité ou de la sécurité. La police doit construire de manière proactive stratégies de prévention pour tenter de résoudre les problèmes, plutôt que de simplement réagir à leurs conséquences néfastes.*
- *Le modèle de statistique informatique est un système de gestion, modélisé à l'origine sur « La théorie des fenêtres brisées », de Wilson et Kelling (1982) selon laquelle les infractions mineures sont traitées afin de réduire crimes. Sur la base de l'analyse des statistiques des crimes déjà commis, chaque commandant de la force publique locale est responsable de la réalisation des actions locales en conséquence.*

(OSCE Guidebook Intelligence-Led Policing, 2017)

Comme le définit William Bratton, responsable successivement des départements de police de Boston, New York et de Los Angeles, la police prédictive : « *C'est la capacité de prédire où le prochain crime sera commis et la capacité de prendre des mesures pour empêcher sa survenue.* ». L'objectif est d'empêcher la survenue de l'événement pour limiter les interventions, les enquêtes et les incarcérations (Bratton, 2011). Cette définition correspond à une vue réduite de l'exploitation des données par la police en la limitant à la prédiction de crimes. Dans cette vue réduite, la méthodologie de la police prédictive est de relier explicitement la probabilité d'occurrence d'un crime ou d'un délit à une zone géographique de survenue. Cette vue ne prend pas en compte l'intervention de la police dans l'environnement qui peut être de trois genres selon Pascal Martens :

- générique, qui vise à affecter des ressources aux zones présentant un risque accru de criminalité.
- spécifique à la criminalité et concerne les interventions basées sur les caractéristiques de la criminalité.
- complexe et se concentre sur le problème et vise à aborder les facteurs qui poussent le risque de criminalité. (Martens, 2017).

Dans cette vision réduite, il s'agit de donner aux policiers la maîtrise de l'information sur seulement trois types de données : type de crime, lieu du crime, date et heure du crime, pour

qu'ils puissent adapter leurs patrouilles et dissuader les criminels de passer à l'acte (Meijer et Wessels, 2019).

L'utilisation des statistiques sur les données criminelles ou d'activité des forces de l'ordre n'est pas nouvelle en soi. Cette vision de la police prédictive applique des principes de contrôle de gestion pour une optimisation de la mise en rapport entre des moyens (effectifs, fréquence de patrouille) et des besoins (présence policière, couverture de zone à risque). Les algorithmes vont s'appuyer sur l'historique des services de police pour bâtir un modèle prédictif sur la base de statistiques et de probabilités. Les résultats obtenus à la suite des différentes expérimentations conduites montrent une tendance à la baisse des crimes et vols. Comme il s'agit d'une vision réduite et donc plus facile à combler, la plupart des solutions logicielles éditées dans les années 2005-2015 se limitent à la corrélation des données internes à la police et leur intégration sur une carte pour faire des *predictive heat map*s, des cartes de chaleurs évolutives dans le temps.

Cette approche limitée à la prédiction et à la géolocalisation est également celle testée en France par la gendarmerie nationale, selon une réponse fournie par le ministère de l'Intérieur à une question de la députée Perol-Dumont : « *L'objectif recherché est la constitution d'une aide à la décision (« analyse décisionnelle »), au profit du commandant d'unité territoriale, notamment à des fins de prévention de la délinquance. Cette exploration s'appuie sur des méthodes scientifiques d'analyse de données issues des statistiques d'infractions constatées par les forces de l'ordre, de données institutionnelles et de données publiques décrivant le territoire dans lequel ces infractions ont été constatées. Le modèle devra être en mesure d'apporter des réponses correspondant à différents critères de temps (année, mois, semaine, jour) et d'espace (département, arrondissement, commune, îlots regroupés pour l'information statistique), afin de permettre la révélation du ou des modèles le (s) plus pertinent (s) pour le territoire.* » (Sénat, 2016). Comme le précise le Général Lizurey, directeur général de la gendarmerie nationale, lors de son audition par la commission de la défense nationale et des forces armées en octobre 2018 : « *En alimentant en données relatives à la criminalité, au contexte socio-économique, mais aussi à la météorologie et à toutes sortes d'autres domaines, une application fonctionnant grâce à un algorithme, nous obtenons une sorte de « carte des températures » de la délinquance. […] Sur la base des informations fournies par le dispositif d'analyse décisionnelle, qui indique où et dans quel créneau horaire des cambriolages sont le plus susceptibles de se produire, le commandement local peut organiser ses patrouilles en concentrant les effectifs là où ils sont le*

plus utiles. Les compagnies de gendarmerie disposent ainsi d'un outil de prévision qui les aide dans leur conception de service ». (Assemblée Nationale, 2018 c).

Si la position de la France est plus nuancée que celle des pays anglo-saxons, dans le sens où l'outil logiciel apporte seulement une aide à la décision et non pas une prédiction, sa restriction à une analyse spatiotemporelle des événements connus correspond à la vision réduite de la police prédictive et ne permet pas l'exploitation de l'ensemble des données auxquelles ont potentiellement accès les policiers. La mise en valeur des données et leur exploitation logicielle sont au cœur des modèles de police prédictive (*predictive policing*) et de police basée sur le renseignement (*intelligence-led policing*). La police basée sur le renseignement (ILP), par définition, correspond à une autre vision de l'exploitation des données, axée sur l'intervention plus que sur la prédiction. C'est sur ce point que les concepts de police prédictive et de police basée sur le renseignement diffèrent le plus. L'ILP est soutenue par l'OSCE (Organisation pour la sécurité et la coopération en Europe) qui souhaite renforcer la sécurité et la stabilité dans la zone Europe afin de prévenir au maximum l'activité criminelle. L'ILP est présentée comme un modèle moderne et proactif qui combine le renseignement, l'évaluation et l'analyse.

Le renseignement n'est pas uniquement destiné à la prévention. Dans sa définition d'origine, militaire, il sert trois objectifs : surveillance et analyse des menaces pour la prévention ; appréciation et suivi de situation pour la manœuvre des forces ; connaissance de l'ennemi et de son environnement, reconnaissance, éclairage pour les opérations et leur préparation, comme le précise Francis Beau : « *le renseignement a pour fonction de fournir l'information utile à l'action (ou à la décision). Sa mission, la tâche qu'il remplit au profit de l'acteur opérationnel qui l'emploie, est la recherche et l'exploitation de l'information nécessaire pour lui faire connaitre toute donnée nouvelle utile à la solution de ses problèmes stratégiques et à l'exercice opérationnel de son activité.* ». Lorsqu'il l'applique au domaine du renseignement intérieur, il transcrit la mission renseignement de la façon suivante : « *la mission dévolue à la fonction renseignement est donc l'interrogation minutieuse (recherche) de l'environnement sécuritaire, c'est-à-dire la surveillance d'un domaine d'opération couvrant tout le champ des activités illégales afin d'en connaitre tous les développements et savoir les menaces qu'ils représentent ou les opportunités qu'ils recèlent (analyse). Sa finalité est d'éclairer l'action policière (domaine d'application) qui a, quant à elle, pour fonction de déjouer les menaces en en protégeant les victimes potentielles (prévention) et de profiter des opportunités pour les combattre (répression)* (Beau, 2019). Même s'il mentionne l'action policière, il restreint la portée de sa définition au domaine d'emploi de la DGSI, nous pensons que cette définition peut

même s'étendre au domaine policier dans son ensemble et qu'elle peut être déclinée jusqu'à la plus petite entité d'emploi qu'est le commissariat au même titre que la fonction renseignement est déclinée jusqu'à chaque unité des forces armées. C'est seulement quand l'action de chaque enquêteur, de chaque policier est menée par le renseignement que l'on peut légitimement parler de police guidée par le renseignement (intelligence-led policing).

Limiter la fonction renseignement au plus haut niveau de synthèse, aux organes de centralisation ne permet d'avoir l'effet recherché sur le terrain. D'ailleurs c'est à partir du terrain, des sources, que nous avons travaillé afin de comprendre les besoins en capacité d'analyse des polices européennes pour mettre en place des processus d'intelligence-led policing.

Nous avons pu étudier trois appels d'offres restreints et confidentiels pour mieux comprendre l'expression de besoin de forces de l'ordre en termes d'exploitation de données (Interpol, 2018 ; Police belge, 2018 ; Police allemande, 2019). Ces appels d'offres et les échanges liés, combinés à des entretiens effectués en France auprès de la Préfecture de Police et de la direction régionale de la police judiciaire de Versailles ont permis de dégager des fonctions clés requises par les forces de l'ordre. Or ces fonctions sont clairement du domaine du renseignement et pas de l'analyse prédictive. La fonction renseignement regroupe plusieurs types de renseignements comme le définit la doctrine interarmées numéro 2 « Renseignement d'intérêt militaire et Contre-ingérence » :

- ***renseignement de situation*** *: comprend la description de la situation, qui consiste à élaborer une représentation de la localisation, de l'état, de la posture des unités, des systèmes, des acteurs, des installations et plus généralement des différents éléments entravant, s'opposant ou susceptibles de s'opposer à l'action de nos forces. L'évaluation de la situation qui complète cette description par une estimation des intentions des acteurs et une analyse prédictive de l'évolution de cette situation.*
- ***renseignement de documentation*** *: est constitué du fond documentaire nécessaire à un niveau de commandement donné. Il permet de percevoir des évolutions dans la durée, favorisant ainsi l'accès à la compréhension des phénomènes et événements rapportés.*
- ***productions ciblées*** *: l'appui au processus décisionnel recouvre les travaux d'évaluation spécifiques, notamment les renseignements d'alerte, d'appui à la planification, de ciblage, à caractère technico-opérationnel, de protection de la force incluant les renseignements de sécurité et de sûreté.*

- ***renseignement d'alerte*** *: obtenu au moyen d'indicateurs ayant valeur d'indices révélateurs de changement de situation. Ces indices peuvent résulter d'Anomalies pouvant avoir valeur d'indices d'alerte (APAVIA) ou bien du franchissement de certains seuils par des indicateurs. Il nécessite des cycles d'élaboration réduits dans le temps et un circuit de diffusion rapide vers l'autorité qui doit le prendre en compte.*
- ***renseignement d'appui à la planification*** *: recouvre les évaluations de renseignement produites pour appuyer le processus de planification prédécisionnelle et opérationnelles. Cette catégorie de renseignement recouvre l'Appréciation de renseignement et la Préparation renseignement de l'espace opérationnel.*
- ***renseignement de ciblage*** *: recouvre tous les renseignements permettant de caractériser et de localiser un objectif ou un ensemble d'objectifs, d'en connaître la vulnérabilité et l'importance relative.*
- ***renseignement technico-opérationnel*** *: recouvre la connaissance technique d'un objet ainsi que la compréhension et l'analyse des situations et des activités observées afin de déterminer le niveau de menace et d'anticiper les intentions adverses.*
- ***renseignement pour la protection de la force*** *: est constitué de l'ensemble des évaluations des vulnérabilités de nos forces armées et de leurs installations face aux actions de l'adversaire ou d'individus ou groupes de toutes natures, susceptibles de les menacer directement ou indirectement ou de contrarier l'exécution de la mission qui leur est confiée.*

  (CICDE, 2010 a).

Chacun de ces types de renseignements correspond à des fonctions requises par les forces de l'ordre souhaitant mettre en place une police menée par le renseignement (intelligence-led policing). Ci-après des illustrations de cas pratiques issus de nos entretiens et étude documentaire.

- Renseignement de situation :
  - Détection d'une vague de criminalité spécifique : ce cas d'utilisation permet de détecter si le nombre de crimes d'un certain type pourrait refléter une vague de criminalité d'un certain groupe. Il permettrait d'identifier si la proximité géographique et temporelle des crimes correspond à un modus operandi.

- Hotspotting : Les points chauds de la criminalité sont signalés par le logiciel, sur la base de données historiques. Les zones désignées comme points chauds peuvent être réorganisées ou les patrouilles peuvent décider de se concentrer davantage sur ces zones. Il donne au chef de la zone de police une vue d'ensemble de sa zone telle que les crimes et le nom de la rue et l'évolution (par heure, jour, semaine selon le type d'infraction) d'une situation.

- Image opérationnelle commune : fournir aux organisations partenaires les conclusions relatives à deux ou plusieurs entités qui sont considérées comme identiques d'après l'analyse des données et pour lesquelles les données biométriques ne permettent pas de confirmer la correspondance. L'objectif est d'encourager la collaboration en vue de l'échange d'informations sur les cibles pour lesquelles tous ont un intérêt direct à interpeler, rechercher, localiser, etc.

- Renseignement de documentation :
  - Résolution d'entité : détecter tous les éléments d'information contenus dans un texte automatiquement et disposer d'un système permettant de détecter dans un ensemble de textes les entités en double et de les fusionner, mais uniquement si les entités ont les mêmes attributs. Sur la base de ces caractéristiques, cette capacité permet de trouver différentes identités qui sont les mêmes personnes. Type d'entités : identités, emplacements, adresses IP, numéros de carte de crédit, IBAN, numéros de téléphone, documents d'identité, immatriculation des véhicules, nationalités, etc.

  - Identification : Être en mesure d'établir un profil complet du sujet et d'identifier les personnes à partir de renseignements qualitatifs (p. ex., établir des liens entre les pseudonymes et les profils criminels), être en mesure d'effectuer une recherche complète d'une entité ou d'un terme donné afin de déterminer s'il est déjà connu dans le système d'information.

  - Clusterisation de crimes : a pour but de regrouper les éléments d'une affaire qui sont similaires pour rechercher des relations entre eux et découvrir des séries possibles. Les groupes de crimes peuvent être utilisés pour rechercher des suspects : si un crime

dans un groupe est résolu, l'auteur est probablement impliqué dans les autres crimes. Étant donné que les affaires d'un groupe peuvent être fusionnées, les autres ressources sont ainsi libérées pour travailler sur d'autres affaires. De plus, les informations de consolidation aident à résoudre les affaires d'un même groupe.

- Productions ciblées :
  - Analyse de réseau social d'une victime : Le cas d'utilisation permet d'avoir une vue d'ensemble du réseau de la victime ou du suspect. En effet, toutes les données les concernant sont collectées et aident les policiers à les analyser (téléphonie, emails, GPS, relations avec la famille et les amis, médias sociaux...) et aident les policiers à les analyser.

  - Détection des valeurs aberrantes : consiste à trouver des personnes dont le comportement s'écarte d'un comportement "normal" (personnes d'un ménage, âge, taille, antécédents, bureau à domicile ou non, autres matériaux sociodémographiques...), et ce faisant, à trouver des personnes ayant un comportement suspect. Ceci peut être appliqué dans un contexte narcotique pour trouver des consommateurs d'énergie anormaux ou des quantités anormales de déchets et enfin pour détecter les laboratoires de drogues à travers ces éléments externes.

  - Analyse de réseau criminelle pour comprendre la composition et la structure du terrorisme, des organisations criminelles et des groupes du crime organisé, identifier les principaux membres, influenceurs ou coordonnateurs, comprendre les activités auxquelles ils participent (p. ex. trafic de drogues, d'armes, enlèvement, etc.) et leurs voies de communication.

- Renseignement d'alerte :
  - Estimation de violence domestique : l'objectif de ce cas d'utilisation est de détecter la violence domestique pour protéger les victimes. Cela se fait grâce à des indicateurs externes tels que les rapports d'intervention (arguments répétés ou plaintes de bruit rapportées par un voisin, antécédents d'un suspect, ...).

- Suivi des médias sociaux : ce cas d'utilisation fournit une analyse en temps réel des médias sociaux et autres données (IOT, téléphonie) pour savoir où se situent les incidents lors d'un événement/démonstration, où se trouve la foule, si une personne recherchée est présente... L'objectif est de détecter les problèmes et permet aux policiers de réagir rapidement.

- Détection d'anomalies de dépositions : analyser les dépositions de témoins ou de suspects pour détecter les mensonges. Appelée "analyse des déclarations" par le FBI, elle consiste à analyser le(s) rapport(s) écrit(s) d'un suspect et à rechercher les déviations dans les parties du discours. Certains marqueurs peuvent aussi être trompeurs : quelques autoréférences personnelles, des marqueurs de distinction et des mots émotionnels négatifs. Cette analyse indique la nécessité d'une enquête plus approfondie ou qu'un témoin/suspects se présente soit de nouveau entendu sur d'autres éléments de l'affaire.

- Renseignement d'appui à la planification :
  - Analyse systémique : La détection des faiblesses du réseau vise à trouver la meilleure cible dans un réseau afin de le déconnecter. Parfois, un responsable de la commercialisation n'est pas la personne à arrêter en premier, parce que l'analyse permettra d'identifier un grossiste voire un producteur. Cela permet de planifier les opérations à mener : enquête, surveillance, intervention.

  - Identifier les itinéraires de déplacements habituels et émergents et les modes opératoires utilisés par les criminels ou les réseaux sur les routes terrestres, maritimes et aériennes. Les principales conclusions de l'analyse permettront aux agents de mieux planifier les futures opérations de contrôle.

  - Prévision de troubles de manifestation : un modèle permettant de donner un premier conseil à la police locale sur la dangerosité d'un événement futur. Ce modèle est construit à partir d'événements ou de manifestations antérieures et de leurs caractéristiques recueillies par la police, telles que l'organisation / les personnes impliquées, les lieux, les objectifs / les thèmes des manifestations.

- Renseignement de ciblage :
  - Le géoprofilage vise à trouver le domicile du délinquant en analysant sa série de crimes et délit, en se basant, par exemple, sur la minimisation de la distance, l'analyse des facturations détaillées des opérateurs téléphonique (call data records).

  - Détection de site diffusant du contenu illégal : l'objectif de ce cas d'utilisation est de détecter des sites web potentiellement illicites : djihadistes, pédopornographiques, vente d'armes, ... en catégorisant leur contenu. Le modèle (un classificateur) est construit en utilisant des sites Web illégaux connus et des sites Web normaux en entrée. Le modèle est capable de noter les pages web soit en temps réel pour des alertes en direct soit en batch (par exemple toutes les heures, pendant la nuit...). Il permet ainsi aux analystes de se concentrer sur le contenu pertinent à leurs domaines de surveillance.

  - Identifier et visualiser les personnes cibles de haut niveau et leurs réseaux en se basant sur l'information des médias sociaux et sur la fréquence, la qualité et le contenu des interactions des médias sociaux sur les plateformes numériques.

- Renseignement technico-opérationnel :
  - Segmentation du contenu d'ordinateurs, de téléphones, également appelé Digital Forensics : cette segmentation du contenu permet aux enquêteurs d'avoir directement un aperçu rapide de ce contenu : les différents contenus, les liens entre les terminaux, les échanges effectués, leur évolution dans le temps... Par exemple, pour les personnes disparues, il pourrait être intéressant d'enquêter sur de nouvelles relations qui sont apparues avant la disparition.

  - Identifier les liens entre les personnes en se basant sur les appels téléphoniques et les messages stockés dans les pièces à conviction ou les enregistrements de données des appels afin de construire une image des réseaux et des entités liées.

- La détection des signatures chimiques peut être utilisée pour différents types d'infractions : incendies criminels, stupéfiants... Elle permet de trouver des voies de production à la vente de stupéfiants, de regrouper les signatures de drogues pour relier différents cas de composition de stupéfiants, de comparer les chromatogrammes des incendies criminels, d'obtenir la signature chimique d'une bombe faite maison. La détection des signatures chimiques permet de relier des cas qui semblent séparés, mais qui ne le sont pas.

- Renseignement pour la protection de la force :
  - Analyse de sentiment social : ce cas d'utilisation exploitera les médias sociaux pour connaître les sentiments des gens à l'égard de la police. Il permet d'adapter et d'améliorer la communication avec la population ; la sécurité des agents (par exemple lors d'une manifestation pour éviter les jets de pierres).

  - Surveillance temps-réel : ce cas d'utilisation fournit une analyse en temps réel des médias sociaux et autres données (IOT, téléphonie) pour savoir où se situent les incidents lors d'un événement/démonstration, où se trouve la foule, si une personne (non)recherchée est présente ; si le public est informé et diffuse une intervention ou son imminence (arrestation à risque d'un terroriste), ... L'objectif est de détecter les problèmes et permet aux policiers de réagir rapidement.

  - Analyse du stress post-traumatique policier : L'analyse avancée peut aider les ressources humaines en analysant les PV fournissant des informations sur une situation traumatique, sur les interventions génératrices de stress. Informés, les cadres sont capables de réagir et d'éviter trop d'absentéisme et de classer les personnes qui ont besoin d'aide avant leur épuisement.

Ces cas d'usages servent à illustrer le fait que le renseignement n'est pas une simple exploitation des données. Il répond à des missions d'échelon variable, de l'opérationnel (préparation à une arrestation d'un criminel dangereux) au stratégique (évolution des cambriolages dans une région), et doit être une fonction transverse à toute la voie hiérarchique. Dans les forces armées, le renseignement n'est pas l'apanage de la seule direction du renseignement militaire, chaque

unité à une fonction de renseignement, chaque soldat est un capteur. Pour mettre en œuvre une politique d'intelligence led-policing, il faut décliner celle-ci dans toutes les unités. Chaque service de police dispose d'une grande quantité d'informations capitalisées depuis des années. Cette masse documentaire constitue en quelque sorte l'historique des services et pourrait servir de base pour entraîner les algorithmes (machine learning) et implémenter les règles métier. Trois structures (environnement criminel, renseignement et décideur) et trois processus (interprétation, influence et impact) sont identifiés comme étant nécessaires au fonctionnement d'un modèle d'ILP. L'intelligence-led policing, bien qu'étant un cadre de maintien de l'ordre qui s'appuie sur des méthodologies antérieures, telles que la police de proximité, la police axée sur les problèmes, les modèles de partenariat du maintien de l'ordre, dépasse l'objectif d'une police basée sur l'analyse statistique sans tomber dans l'argument commercial de la police prédictive. Face à la profusion toujours plus grande d'information, le besoin d'une solution capable d'assister les forces de l'ordre dans leur travail d'investigation et de sécurisation n'est plus à démontrer.

8.3. L’exploitation de données pour une police guidée par le renseignement

Afin de mettre à la disposition des forces de police des capacités modernes pour combattre et prévenir la criminalité, il faut une plateforme d'analyse en mesure de combler les lacunes déjà identifiées dans la gestion, le traitement et l'analyse des sources de données structurées et non structurées auxquelles elle a accès. Nos travaux ont porté notamment sur le développement d’une telle plateforme : la solution « Détection et Investigation », conçue pour fournir un traitement de bout en bout le plus complet du marché en matière de gestion, de détection, d’évaluation, de suivi, de catalogage, d’alerte et de signalement de données. Le système utilise des modèles de comportement connus pour prévoir les menaces émergentes tout en apprenant des comportements nouveaux et inconnus susceptibles d’être des anomalies ayant valeur d’alerte. Il automatise le processus de détection afin qu'il soit possible d’identifier les risques et menaces plus rapidement, plus précisément et plus efficacement. A travers un outil global, l’analyste est capable de faire le lien entre la vue macro et la moindre donnée en détail grâce à des outils de visualisation, d’exploration et de mesure mettant en valeur les données dans une grande autonomie et dans un délai de réponse raisonnable. Étant donné que les modes opératoires et capacités adverses évoluent constamment, la solution fournit des alertes et des informations aux experts des différents domaines de manière à ce qu'ils puissent prendre les meilleures décisions plus rapidement que jamais. Ils seront en mesure de créer du renseignement exploitable pour éclairer la prise de décision des autorités, appuyer l’intervention, tout en apprenant de nouveaux modèles et tendances à mesure qu'ils se développent.

La solution est directement applicable, car les processus métier qu’elle soutient sont issus d’un retour d’expérience métier de plusieurs années. Cette solution pourra être utilisée par les différents profils :

- Les analystes / exploitants, utilisateurs principaux de la plateforme pour la production du renseignement ;
- Les spécialistes du traitement de certains médias (images, vidéo, langues, ...), utilisateurs progressifs de la plateforme d’analyse pour l’utilisation de nouvelles

méthodes de traitement (deep learning, …) pour vérifier et affiner les résultats des traitements initiaux sur ces médias ;

- Des utilisateurs opérationnels : enquêteurs, force d'intervention, police de proximité, procureurs, juges, etc.

Les plus-values opérationnelles apportées par la plateforme seront une augmentation accrue du champ de l'analyse et de sa rapidité ainsi qu'une meilleure capacité à anticiper les événements par :

- La capacité à traiter automatiquement, dans une même analyse, de très gros volumes de données (en temps réel ou en temps différé), ce qui permettra d'augmenter la productivité des analystes ;
- La capacité à appliquer des séquences de traitement sur des données de même nature, mais d'origines différentes qui permettra d'élargir le champ de vision des analystes (accès à de nouveaux gisements de données collectées par la distribution des traitements) ;
- La capacité à mettre au point sur un environnement spécifique et déployer rapidement en production de nouveaux algorithmes de traitement, de recherche ou d'analyse des données collectées qui fournira plus rapidement aux analystes les moyens d'en extraire des informations plus précises ;
- La capacité de mettre en œuvre de nouvelles méthodes et de nouveaux algorithmes issus du monde Big Data (Machine Learning, Deep Learning) pour faire apparaître de nouvelles relations ou des corrélations ;
- La capacité à retraiter des données dans le passé et sur de plus grandes échelles de temps pour faire apparaître de nouveaux « patterns » de comportements individuels ou sociaux (regroupements, attroupements, événements simultanés, directions d'appels téléphoniques, …) et de nouvelles corrélations entre des événements ;
- L'utilisation de mécanismes d'apprentissage sur de gros volumes de données qui permettront aux analystes d'anticiper des événements en mettant en évidence des « patterns » de comportements et en les comparant à des situations issues de données fournies en temps réel.

Pour traiter les cas d'usages cités précédemment, les fonctions suivantes doivent être mises en œuvre :

- Accéder, transformer les données transmises et archivées en renseignements, ce qui signifie la mise en œuvre de processus de collecte, d'extraction, transformation et de chargement (ETL), d'exploitation, d'analyse et de diffusion.
  - Tri automatisé des données pertinentes en fonction du sujet d'intérêt de l'analyste ;
  - Recherche complète dans toutes les bases de données et tous les formats (TAJ traitement d'antécédents judiciaires, FPR fichiers des personnes recherchées, FNAEG Fichier national des empreintes génétiques, etc.) ;
  - Alerter les analystes sur les sujets qui les concernent ;
  - Retrouver toutes les informations sur une entité d'intérêt par le biais du système d'information ;
  - Identifier les individus en fonction de leurs caractéristiques personnelles.

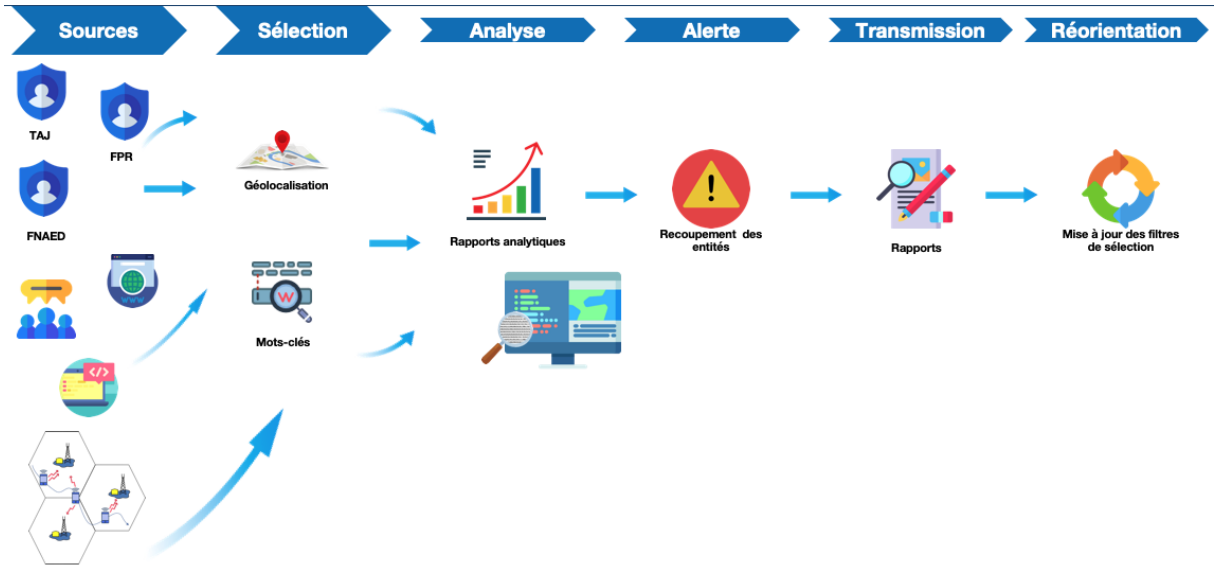


Figure 64 : Schéma d'intégration de données d'une plateforme de renseignement policier

- Analyser en réseau des données liées qui amélioreront la performance globale de références croisées.
  - Analyse des réseaux sociaux de l'organisation criminelle et des affaires criminelles ;
  - Identifier les données similaires et/ou apparentées de manière transparente à travers les référentiels ;

- Mettre en évidence les tendances et les processus criminels afin d'alerter et d'estimer les probabilités de résultats ;
- Effectuer une analyse visuelle du réseau pour comprendre la structure des organisations criminelles ;
- Identifier et visualiser le réseau de personnes d'intérêt sur les réseaux sociaux ;
- Identifier / visualiser un réseau relié par des communications téléphoniques, voire figure 66.

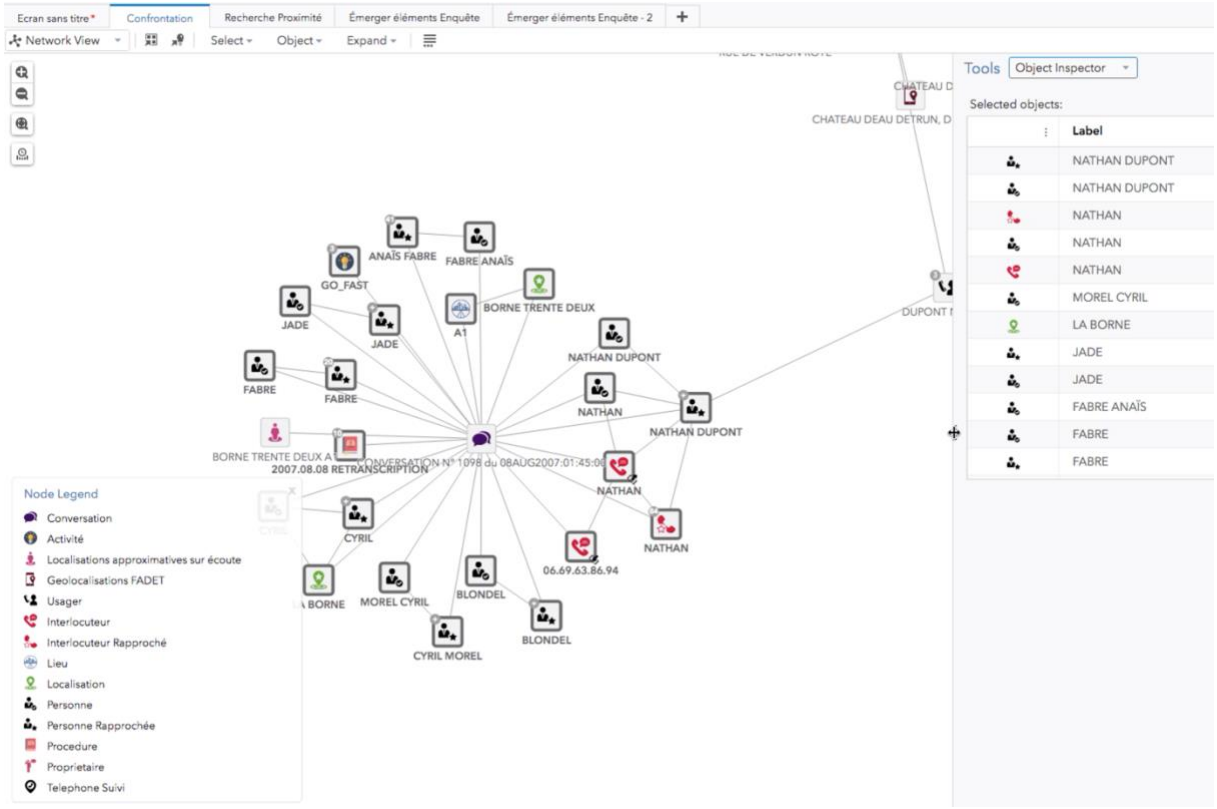


Figure 65 : Analyse de réseau d'une conversation téléphonique

- Analyse géographique pour permettre l'identification transversale des sujets d'intérêt par géolocalisation
  - Identifier les itinéraires et les modèles de déplacement et de trafics, voir figure 66
  - Fournir des cartes thermiques
  - Identifier les similitudes géographiques

- Analyse géographique des itinéraires des terroristes et des combattants étrangers, suivi des activités des différents groupes terroristes dans une zone donnée, voir figure 67
- Analyse géographique des comportements des mouvements de vol, pour détecter les points critiques pour la sécurité

Géolocaliser les adresses IP pour identifier les liens localisés potentiels avec les crimes

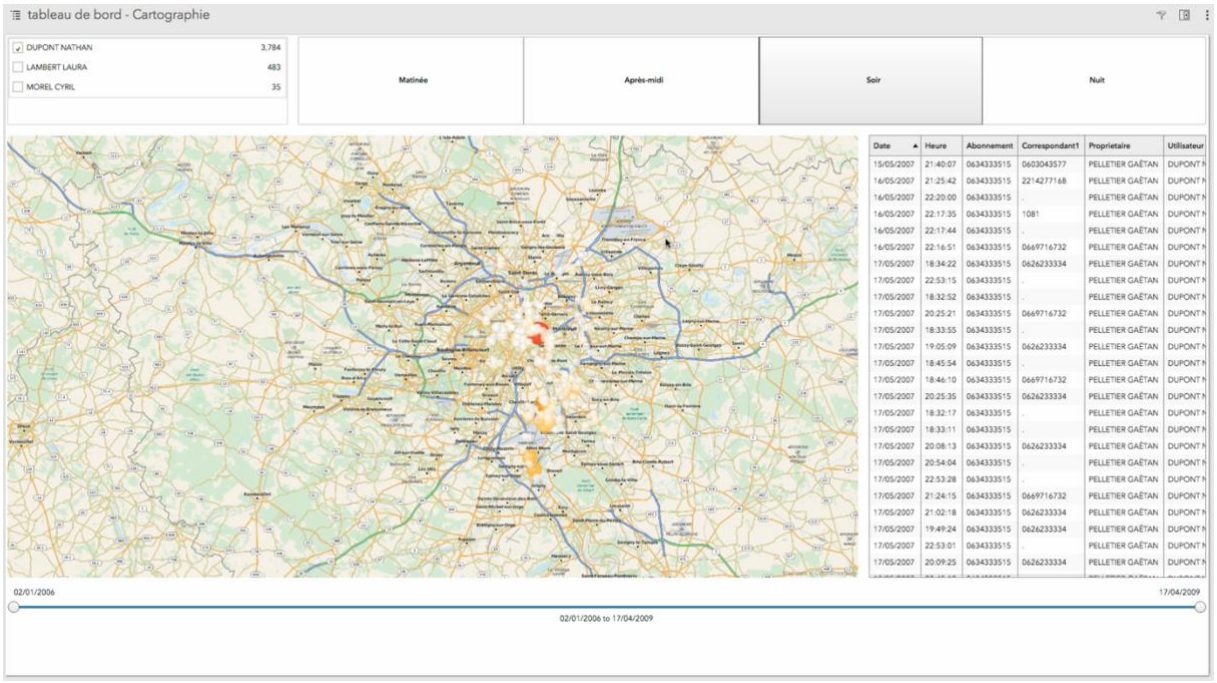


Figure 66 : Identification des séquences d'activités d'un suspect (pattern of life)

- Visualisation des données pour superviser les volumes globaux de données par base de données ou entre bases de données grâce à des statistiques et une sémantique avancée.
  - Identification des points de vue et des séquences d'activité
  - Avertissement de corrélation et de causalité basé sur l'intensité et la fréquence, voir figure 68
  - Améliorer le point de vue global sur les données disponibles par analyste ou par sujet
- Visualisation des transactions financières pour identifier les sources de financement du terrorisme / criminalité

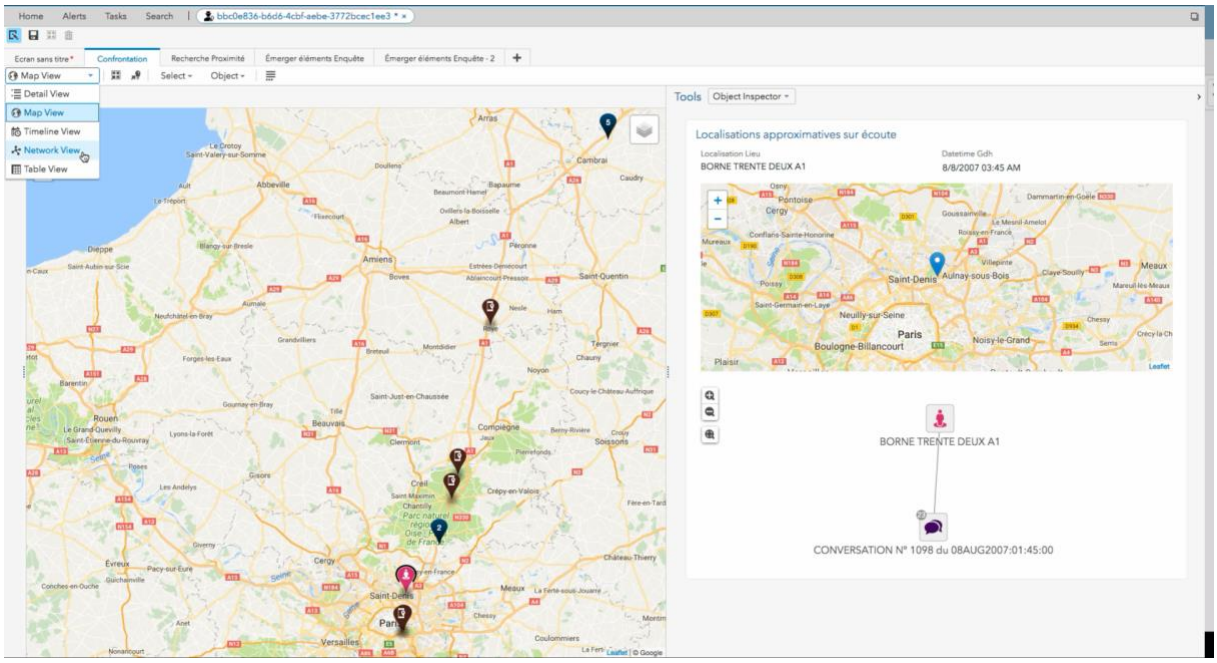


Figure 67 : Suivi des volumes et croissances des appels d'une cible

Figure 68 : Affichage des balises de suivi de position

- Gestion du rendement
  - Identifier les lacunes en matière de capacités
  - Fournir des résultats mesurables du rendement global
  - Fournir des capacités d'établissement de rapports

8.4. Dangers et Limites de la police prédictive, et règles pour l'ILP

Il ne fait aucun doute que la police peut gagner en efficacité par une meilleure exploitation de ses données internes et les données auxquelles elle peut avoir accès. Compte tenu des enjeux du big data regroupés sous l'acronyme 5V pour : volume, vélocité, variété, véracité et valeur, cette exploitation des données doit reposer sur des systèmes de haute performance animés d'algorithmes issus de la data science. Cependant, le contexte policier n'est pas celui d'une entreprise qui doit gagner des parts de marchés ni celui d'une armée en guerre avec un ennemi. L'activité policière est régulée par une législation spécifique, et ses efforts de prévention et de répression peuvent être purement et simplement annulés par décision de justice à la moindre erreur de procédure, c'est-à-dire à la moindre faille dans l'exploitation des données. Depuis 2014, de nombreuses expérimentations ont été menées en particulier aux États-Unis et en Grande-Bretagne. Ces expérimentations de police prédictive se basent sur des modèles statistiques et algorithmes empruntés entre autres à des domaines d'études comme le marketing, l'imagerie médicale ou la sismologie. Une des finalités de cette « police prédictive » était de prépositionner des moyens au plus près des endroits où des délits sont susceptibles d'être commis pour prévenir leur survenue. Ce principe rend de fait le logiciel non évaluable tout en étant un argument commercial, comme l'explique le site internet de PredPol : « *Bien que les boîtes prédictives de PredPol prévoient qu'un crime se produira dans la zone de prédiction, il n'y a aucune garantie qu'un incident ou une arrestation aura lieu. ET C'EST LE BUT ! La présence d'agents de police dans les zones de prévision a un effet dissuasif et de répression, ce qui permet de prévenir la criminalité en premier lieu.* » (Predpol, 2019).

Cependant, certaines expérimentations ont poussé l'exercice plus loin sous l'incitation des promesses des fabricants de logiciels et sont allées jusqu'à cibler des personnes à risque, récidivistes ou identifier des victimes potentielles. Ces profilages algorithmiques ont été décriés, à juste titre, par de nombreux défenseurs des libertés individuelles. Ainsi la police de Chicago utilise un algorithme pour créer une liste des individus stratégiques (Strategic Subject List, SSL). La police de Chicago décrit la SSL de la façon suivante : « *La SSL est une liste par ordre d'importance des victimes potentielles et des sujets ayant la plus grande propension à la violence. Le modèle SSL examine les personnes ayant un casier judiciaire qui sont classées en fonction de leur probabilité d'être impliquées dans une fusillade ou un meurtre, que ce soit en tant que victime ou délinquant, connu sous le nom de "Partie prenante à la violence" (PPV).*

Le logiciel est généré à partir de données empiriques qui énumèrent les attributs du casier judiciaire d'une personne, y compris les antécédents de violence entre associés criminels, la mesure dans laquelle ses activités criminelles sont à la hausse, et les types et l'intensité des antécédents criminels. » (Chicago Police Department, 2015). L'algorithme employé n'est pas public et même s'il utilise strictement des données policières, il n'existe aucune information sur la façon dont elles sont exploitées sur le terrain par les forces de l'ordre (Posadas, 2017).

- Le nombre de fois où un individu a été victime d'une fusillade ;
- L'âge d'un individu lors de sa dernière arrestation ;
- Le nombre de fois où un individu a été victime d'une agression ou d'une agression aggravée ;
- Le nombre d'arrestations antérieures d'un individu pour des infractions avec violence ;
- Le nombre d'arrestations antérieures de stupéfiants ;
- Le nombre d'arrestations antérieures d'un individu pour utilisation illégale d'une arme ;
- Tendance récente de l'activité criminelle d'un individu [1] ;
- Appartenance à un gang.

Selon une enquête du New York Times : « *L'algorithme est utilisé à Chicago depuis plusieurs années et son efficacité est loin d'être claire. Chicago a été à l'origine d'une grande partie de l'augmentation des meurtres en milieu urbain l'an dernier.* (Asher, Arthur, 2017).

Ce programme est associé à un autre programme appelé « Custom Notifications » (notifications personnalisées) programme décrit de la façon suivante dans les directives de la police de Chicago : « *La " notification personnalisée " est un processus qui permet d'identifier les acteurs criminels et les victimes potentielles associées au continuum de la violence. Une fois identifiée, la personne est informée des conséquences qui découleront de la poursuite d'une activité violente. La notification personnalisée est fondée sur une recherche [académique] nationale qui a conclu que certaines actions et associations dans l'environnement d'une personne sont un précurseur de certains résultats si la personne décide de s'engager ou continue de s'engager dans un comportement criminel. La notification personnalisée comprendra une description des options fédérales et étatiques en matière de détermination de la peine, le cas échéant, ainsi qu'une identification de la possibilité de saisir des biens et d'autres conséquences, le cas échéant.* » (Chicago Police Department, Op.cit.).

Ces deux programmes sont caractéristiques des efforts du National Institute of Justice (NIJ) américain en faveur de la police prédictive qui depuis 2009 : « *a octroyé des millions de dollars*

en subventions à tout service de police ayant un programme prédictif en plein essor. La police de tout le pays a fait une demande d'accès à ces dollars du NIJ. » (Stroud, 2014).

L'analyse légale de ce type d'initiative d'une force de police n'est pas en leur faveur : « *Cette analyse révèle plusieurs défauts constitutionnels et statutaires dans l'utilisation actuelle du SSL. La police de Chicago ne peut certainement pas utiliser le protocole SSL comme base de soupçon raisonnable ou comme motif probable. Placer quelqu'un sur la SSL peut constituer une recherche déraisonnable en violation du quatrième amendement, selon la façon dont la doctrine actuelle continue d'évoluer. Le fait de placer quelqu'un sur la SSL viole également le quatorzième amendement en privant cette personne de ses droits à la liberté protégés en matière de confidentialité des informations et en évitant la stigmatisation sans une procédure légale régulière. Enfin, en surchargeant de façon disproportionnée les communautés afro-américaines et latino-américaines de Chicago, l'utilisation actuelle de la SSL a un impact racial disparate en violation de l'Illinois Civil Rights Act.* ». (Tucek, 2018).

Et c'est sans compter sur les critiques portant sur les algorithmes utilisés en police prédictive, l'exploitation des données par la police et l'attribution de responsabilités dans le processus policier et judiciaire.

Les critiques liées aux algorithmes sont essentiellement de deux ordres : en tout premier sur la nature des données utilisées pour construire les algorithmes et bâtir le modèle de données. Or, si les modèles s'appuient exclusivement sur des données propriétaires et confidentielles de la police le risque est que : « *l'information est biaisée par des facteurs autres que ceux qui sont mesurés. Il est beaucoup plus difficile d'identifier les préjugés dans les modèles de prévision de la justice pénale. Cela s'explique en partie par le fait que les données policières ne sont pas recueillies uniformément, et en partie par le fait que les données recueillies par la police reflètent des biais institutionnels de longue date en matière de revenu, de race et de sexe*. » (Dixon, Isaac, 2019). La seconde catégorie de critique porte sur la transparence et l'explicabilité des algorithmes. Sur le point de la transparence : « *les algorithmes qui produisent des jugements bouleversants sur tout, de la libération conditionnelle au crédit, sont souvent eux-mêmes des "boîtes noires* » pour deux raisons : la complexité du code tant pour la personne observée que pour le policier utilisant le système ; l'utilisation de code propriétaire et l'obfuscation (volonté de rendre un code impénétrable pour en protéger la propriété intellectuelle) des sociétés commerciales propriétaire des algorithmes (Joh, 2017). Pour compenser cela des chercheurs développent des algorithmes de détection de discrimination algorithmiques tels que le Quantitative Input Influence (Datta, et al., 2016). Sur *l'explicabilité* de l'algorithme, Lyria

Moses et Janet Chan estiment que le risque est réel que les utilisateurs et cibles des algorithmes, en premier lieu les policiers, les procureurs et les suspects puissent : « *ne pas avoir l'expertise nécessaire pour déduire les biais inhérents au choix de l'algorithme ou du processus d'analyse.* » (Moses et Chan, 2018). La population impactée ne disposant pas de la maîtrise de l'information (au sens de capacité et compétences telles que nous l'aborderons dans le chapitre suivant) pour être en mesure de comprendre les causes et conséquences de l'implication d'un algorithme dans le système judiciaire.

Ce qui amène à la catégorie des critiques liées à l'exploitation des données par la police et de l'externalisation de cette exploitation vers des sociétés privées. La police prédictive lorsqu'elle s'éloigne de la simple géolocalisation d'événements pour aller vers le profilage de criminels et de victimes potentielles change la façon de travailler de la police. Tout d'abord pour faire du profilage la police doit avoir accès à un très large jeu de données qui dépassent le cadre strict des données policières et incluent des données personnelles. Or, la réglementation européenne relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales est très stricte dans ce domaine quant au risque de discrimination suite à l'utilisation de données personnelles : « *Tout profilage qui entraîne une discrimination à l'égard de personnes physiques sur la base de données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux, devrait être interdit en application des conditions établies aux articles 21et 52 de la Charte*. » (Parlement Européen, 2016). Du positionnement d'une patrouille dissuasive, on passe à une arrestation préventive. Cette tendance au préventif, lorsqu'il se rapproche du concept militaire de frappe préventive, est un risque reconnu (Andrejevic, 2017). De plus, la question de la responsabilité dans le processus de décision est également posée comme un risque conséquent à l'utilisation des algorithmes de prédiction : « la tentation est d'externaliser certains aspects du processus décisionnel, et donc la responsabilité et l'obligation de rendre compte de la décision elle-même, vers des outils technologiques. » (Moses et Chan, op. cit.). Les défenseurs de la liberté individuelle sur l'internet de la Electronic Frontier Foundation vont même jusqu'à faire dire à l'un de leur avocat, Hanni Fakhoury, : « *Je crains que ces programmes ne créent un environnement dans lequel la police peut se présenter à la porte de n'importe qui à n'importe quel moment et pour quelque raison que ce soit* ». (Stroud, op. cit.).

Enfin, la troisième nature de critiques à la police prédictive est la responsabilité des actions et la *mésurabilité* des résultats dans l'environnement sécuritaire. L'utilisation d'un logiciel pour

conduire l'action policière pose le problème de l'attribution des responsabilités notamment dans le cas d'erreurs de ciblage. Cette attribution est rendue difficile par l'absence de maîtrise des algorithmes précédemment cités, mais aussi par l'absence d'accès aux données policières : « si *les données policières demeurent privées ou classifiées, le comportement des agents et les tactiques policières ne peuvent être examinés de près et tenus responsables par le public. Les ministères pourraient utiliser les données pour légitimer des interventions problématiques, comme la surveillance et les arrêts injustifiés, et pour réduire au silence le débat public sur l'éthique des tactiques policières.* » (Shapiro, 2017).

Par ailleurs, il demeure très difficile d'établir une relation de cause à effet entre la mise en place de ces programmes et la diminution de la criminalité qui peut être imputée à d'autres facteurs comme le remarque Nick Corsaro, professeur à l'Université de Cincinnati. Ce dernier a contribué à la construction de la base de données sur les gangs du New Orleans Police Departement et a également travaillé sur une évaluation programme « CeaseFire » de la Nouvelle-Orléans. Il a constaté que le déclin global des homicides à la Nouvelle-Orléans coïncidait avec la mise en œuvre du programme « CeaseFire » par la ville, mais que les quartiers du centre-ville visés par le programme « *n'ont pas connu de baisses statistiquement significatives correspondant à la date de début novembre 2012* ». (Corsaro, 2015). En clair, l'étude n'a pas confirmé les affirmations de Palantir et des autorités municipales selon lesquelles des interventions reposant sur des données étaient à l'origine de la baisse temporaire du nombre de crimes violents. De plus certains crimes sont plus prévisibles que d'autres notamment ceux qui demandent un certain niveau de préparation, or ce sont ces crimes dont la prévention est la plus facilement mesurable (Bachner, 2014). Ainsi il paraît difficile de mesurer l'efficacité d'une opération de police prédictive, a fortiori si le crime n'a pas eu lieu pour cause de prévention.

8.5. Conclusion

La police prédictive, et ses chantres ont su générer de l'intérêt pour l'exploitation des données au moyen d'algorithmes par la police. En s'éloignant du concept initial d'exploitation logicielle des données et par la diffusion d'une vision restreinte limitée à la géolocalisation spatiotemporelle de crime pour en prédire les occurrences futures, elle a montré des résultats limités, causé de nombreux doutes et déçu certains praticiens. Le renseignement quant à lui est une fonction essentielle de la conduite des opérations militaires, son imbrication dans tous les processus et son efficacité ne peuvent être remises en cause. Si la police prédictive se préoccupe d'où et quand le crime peut se produire, la police guidée sur le renseignement, qui peut comprendre une part de prédiction statistique, met l'accent sur la prévention de la victimisation et l'investigation en passant par une implication des forces de l'ordre sur le terrain et par l'entretien d'un dialogue avec la population pour un recueil permanent d'information. Selon le ministère de la Justice américain, les méthodes de police axées sur le renseignement (ILP) constituent « *une approche collaborative de l'application de la loi combinant maintien de l'ordre, résolution des problèmes (problem-solving policing), échange d'informations [entre services] et responsabilisation de la police, auquel s'ajoutent des opérations de renseignement améliorées* » (U.S. Department of Justice, 2009). Avec l'amélioration de la technologie, les services de police disposent de modèles de données de plus en plus performants, conçus pour détecter les habitudes et les récurrences en tirant parti des données issues de différentes sources internes, techniques ou documentaires, et en intégrant l'espace et le temps. En d'autres termes, pour être en mesure d'exploiter pleinement le potentiel de l'exploration de données pour le maintien de l'ordre, il faut adopter une approche aussi holistique que possible. Cela signifie que le maintien de l'ordre axé sur les données consiste à recueillir des données à la plus grande échelle possible et à interconnecter le maximum d'ensemble de données afin d'obtenir des renseignements exploitables qui permettront de lutter efficacement contre la criminalité - une criminalité qui, dans certains cas, ne s'est pas encore révélée. (Egbert, 2019). La mise en œuvre de cette capacité n'est cependant toujours pas d'actualité en France : « *La France - à l'instar de ses voisins - ne peut plus se permettre l'économie d'une alternative telle que le modèle de police guidée par le renseigne- ment. En la matière, le système policier français a aujourd'hui fait le choix d'avancer par petits pas, sans heurter notre approche si singulière des questions de sécurité. Mais pour ne pas demeurer une simple mode, il lui reste encore à définir une véritable doctrine de renseignement criminel à la française* » (de Maillard, 2014).

9. Chapitre 9 : la maîtrise de l'information

9.1. Introduction

L'internet est reconnu par les plus grandes instances mondiales comme étant l'un des facteurs clé du développement durable global. Selon l'agence des télécommunications des Nations Unies, citant l'Union Internationale des Télécommunications, 51,2 % de la population mondiale, soit 3,9 milliards de personnes, est connectée depuis décembre 2018 (UN Telecoms Agency, 2018). De nombreuses initiatives, publiques comme privées, sont mises en œuvre pour connecter le reste de l'humanité, développer l'accès haut débit et réduire la fracture numérique qu'elle soit liée au genre, à la richesse ou à la géographie. L'importance des efforts consacrés à cette technologie est justifiée par son rôle unique pour le développement de l'individu comme de la société. Cependant cette nouvelle capacité technologique, unique dans l'histoire de l'humanité pour certains, requiert plusieurs niveaux de maîtrise, parfois contestés. Ce chapitre va aborder la notion de maîtrise de l'information selon trois points de vue, trois rôles que nous occupons concomitamment, celui d'individu, de citoyen, et d'utilisateur de l'internet. Tout d'abord, nous aborderons le principe de maîtrise de l'information en général au niveau élémentaire, individuel, indépendamment du medium de ladite information. La définition même du concept est sujette à débat, même si l'on constate une forme de convergence vers un concept de maîtrises multiples sous l'appellation de *translittératie*. Cette translittératie nécessaire à la maîtrise de l'information pour un individu s'inscrit dans des environnements non neutres que sont les médias en général et l'internet en particulier. L'éducation aux médias est donc un autre facteur essentiel pour l'individu, mais aussi pour la société, tant ces derniers ont un impact reconnu sur la démocratie même. En effet, l'imbrication de l'internet dans la vie de la cité fait que la maîtrise de l'information affichée à un citoyen est facteur de puissance ou de déstabilisation, interne comme externe. Au-delà des aspects éducatifs, la maîtrise de l'information sur le web repose également sur la gouvernance globale et la neutralité de celui-ci. Ses impacts sécuritaires et économiques globaux comme locaux font que sa gouvernance est l'objet de lutte entre toutes ses parties prenantes, qu'il s'agisse d'organisations intergouvernementales, de nations, comme d'entreprises privées. La problématique de la

défense des intérêts de l'individu, du citoyen, et de l'utilisateur suit des chemins divergents en fonction de l'interlocuteur qui cherche à y apporter une réponse.

9.2. Maîtrise de l'information et besoin individuel

On doit à l'American Library Association (ALA) la première formulation de l'idée d'une « information literacy », traduite en français par « maîtrise de l'information » pour les uns (Horton 2007), « culture de l'information » pour les autres. Fondée en octobre 1876 elle a pour mission de : « *diriger le développement, la promotion et l'amélioration des services de bibliothèque et d'information et de la profession de bibliothécaire afin d'améliorer l'apprentissage et de garantir l'accès à l'information à tous* » (American Library Association, 2019). Elle anime donc une profession, celle de bibliothécaire, qui est un soutien important à la recherche scientifique, mais qui joue aussi un rôle éducatif (de l'école primaire à l'université) tout aussi important que celui des enseignants aux États-Unis. Ce rôle éducatif dépasse d'ailleurs le milieu scolaire et universitaire ; il concerne également l'ensemble de la population à travers le réseau des bibliothèques publiques. Forte d'environ 60 000 membres, son influence est certaine. Par des conférences et de plans pluriannuels, cette association a contribué à définir et standardiser des concepts clés des sciences de l'information et de la communication portant sur la maîtrise de l'information. Preuve s'il en fallait de l'influence de cette association, ses définitions ont influencé des organisations comme l'Unesco dans leur définition du concept.

L'ALA définit la maîtrise de l'information (information literacy) comme un ensemble de capacités et de compétences qui permet aux individus de « *reconnaître le moment où l'information est nécessaire et à avoir la capacité de localiser, d'évaluer et d'utiliser efficacement l'information nécessaire ». Pour maîtriser l'information, il faut donc posséder des compétences non seulement en recherche, mais aussi dans le domaine de la pensée critique.* » (American Library Association, 2017 a). Cet ensemble capacité/compétence est conçu à l'échelle individuelle et n'est pas défini, initialement, dans un contexte. Il s'agit d'une fonction générique à traiter de l'information, elle se distingue donc d'une fonction technique qui est celle d'adapter cet ensemble capacité/compétence dans un environnement particulier comme peuvent l'être une librairie, une base de données, un média social.

Cependant, un individu agit dans des environnements informationnels multiples simultanés, et aujourd'hui la maîtrise de l'information ne se distingue plus d'une certaine forme de maîtrise technique. L'Unesco inscrit la maîtrise de l'information dans un contexte qui dépasse l'individu. Dans sa proclamation d'Alexandrie (2005) sur la maîtrise de l'information et l'apprentissage tout au long de la vie, il est indiqué que : « *La maîtrise de l'information est au*

cœur de la formation tout au long de la vie. Elle permet aux gens, dans tous les chemins de la vie, de chercher, d'évaluer, d'utiliser et de créer l'information pour des objectifs personnels, sociaux, professionnels et éducationnels. C'est un droit humain de base dans un monde numérique qui apporte l'intégration de tous les peuples. (Unesco, 2005). L'Unesco définit la maîtrise de l'information comme droit humain fondamental et l'inscrit dans deux contextes : *la formation tout au long de la vie* et surtout *le monde numérique*. La notion de formation tout au long de la vie montre que la maîtrise de l'information à titre individuel dépasse le champ scolaire. En effet, nombre d'individus ne se sont pas en mesure d'atteindre le niveau scolaire nécessaire pour obtenir l'ensemble capacité/compétence susmentionné, mais sont potentiellement en mesure de l'acquérir plus tard dans leur vie ou en dehors du périmètre scolaire, encore faut-il qu'existent des infrastructures qui le permette.

Comme le montre la définition de l'Unesco et d'autres que nous verrons ci-après, le monde numérique est désormais indissociable de la maîtrise de l'information. C'est pourquoi, sous le concept *maîtrise de l'information*, dans son acceptation la plus globale, plusieurs formes de *maîtrises* sont imbriquées (Bawden, 2001) : la maîtrise de l'information (information literacy) ; la maîtrise des technologies de l'information (Computer literacy), la maîtrise des bibliothèques (library literacy) ; l'éducation aux médias (Media literacy) ; la maîtrise de l'internet (network literacy) ; maîtrise du numérique (Digital literacy). Plutôt que de les mettre en concurrence, nous avons tout intérêt à fusionner ces maîtrises ou littératies comme le propose Olivier Le Deuff, pour qui : « *les littératies informationnelles, médiatiques, numériques sont en train de passer d'une situation de concurrence à une perspective de convergence en matière de formation.* » (Le Deuff, 2012).

D'ailleurs lorsqu'on prend la définition de l'ALA sur la maîtrise du numérique, on voit que celle-ci se recoupe avec celle de la maîtrise de l'information tellement ces concepts sont liés aujourd'hui : « *la maîtrise numérique implique de connaître les outils numériques et de les utiliser de manière communicative et collaborative par le biais de l'engagement social. La culture numérique est « la capacité à utiliser les technologies de l'information et de la communication pour trouver, évaluer, créer et communiquer des informations, nécessitant à la fois des compétences cognitives et techniques ».* (American Library Association, 2017 b). Cette fusion ou imbrication de compétences se retrouve dans le concept de *translittératie* tel que le définit Sue Thomas : « *La translittératie est la capacité de lire, d'écrire et d'interagir sur une gamme de plateformes, d'outils et de supports allant de la signature à l'oralité, en passant par l'écriture manuscrite, l'impression, la télévision, la radio et le film, en passant par les réseaux*

sociaux numériques », elle associe ce concept à un autre dont il semble indissociable, celui de *nouveaux médias*. (Thomas et al., 2007).

Le sujet de l'éducation est d'autant plus complexe que les premiers concernés, les élèves, sont souvent considérés comme étant une génération native du numérique (Digital Natives), c'est-à-dire de jeunes ayant connu le monde numérique dès leur naissance et par extension le maîtrisant mieux que les générations précédentes, voire, mieux que leurs enseignants. Il ne faudrait pas faire l'erreur de confondre utilisation et maîtrise : « *Étant donné que les jeunes filtrent quotidiennement des millions d'informations au fil de leur participation au monde en ligne, l'argument est souvent que ces nouvelles générations sont des natives du numérique et qu'elles sont technophiles voire maitrisent l'information. Il est peut-être vrai que les jeunes sont des consommateurs habiles d'informations et trouvent qu'il est plus naturel d'interagir virtuellement qu'en personne, mais cela ne signifie pas pour autant qu'ils comprennent les médias avec lesquels ils s'engagent ou ce qu'ils représentent.* » (Stoddard, 2014). Avec 20 années d'expérience dans l'évaluation de compétences informatiques, l'entreprise sociale à but non lucratif European Computer Driving Licence membre de la Fondation International Computer Driving Licence, met en œuvre des programmes de certification numérique avec près 2,5 millions de tests effectués annuellement. Cette dernière dans un document datant de 2014 confirme cette erreur d'appréciation :

- *Le terme « natif numérique » suggère faussement que les jeunes savent intuitivement comment utiliser les technologies numériques. Ce terme perpétue la perception de certains parents, enseignants et décideurs politiques et conduit à l'omission des compétences essentielles dans les programmes scolaires.*
- *Les preuves montrent que l'exposition à la technologie ne peut être assimilée à la capacité de l'utiliser. En fait, un pourcentage substantiel de jeunes dans les pays européens n'a pas les compétences de base en TIC.*
- *Les jeunes ont tendance à surestimer leur niveau de compétences numériques. Des tests pratiques indiquent que, même si leur confiance est grande, leurs compétences en matière d'utilisation des ordinateurs et d'Internet sont loin d'être complètes.* (ECDL, 2014).

En France, le concept de translittératie s'inscrit dans un champ éducatif appelé l'éducation aux médias et à l'information (EMI) mis en œuvre par la loi d'orientation et de programmation pour la refondation de l'École de la République, où il est stipulé que l'éducation nationale, au primaire « *contribue également à la compréhension et à un usage autonome et responsable des*

médias, notamment numériques. ». Au collège : « *l'éducation aux médias, notamment numériques, initie les élèves à l'usage raisonné des différents types de médias et les sensibilise aux enjeux sociétaux et de connaissance qui sont liés à cet usage.* » (Assemblée nationale, 2013). Cette EMI se donne pour but de : « *permettre aux élèves d'exercer leur citoyenneté dans une société de l'information et de la communication, former des "cybercitoyens" actifs, éclairés et responsables de demain.* (Eduscol, 2019). Inscrit dans la loi d'orientation de l'Éducation nationale, cette inclusion d'une EMI dans tous les cycles et son inscription dans le parcours citoyen est en accord avec la stratégie recommandée par l'Unesco qui préconise notamment de cibler les : « *Ministères de l'Éducation ; Associations de bibliothèques; Conseils d'enseignants professionnels; Commissions scolaires, facultés d'éducation; Départements des médias et de la communication et des bibliothèques et de l'information, etc.*» (Unesco, 2013 a). Même si de nombreux efforts restent à faire selon conseil national d'évaluation du système scolaire : « *l'institution scolaire ne paraît pas, pour autant, pleinement accompagner les jeunes dans un univers informationnel en mutation marqué par des débats forts autour des réseaux sociaux et des infox qui s'y propagent. Ainsi, l'éducation aux médias, en tant qu'objet d'étude, n'est abordée que dans la moitié des collèges et lycées. Celle-ci semble se résumer, le plus souvent, à une éducation par les médias (en utilisant des supports d'information de type article de journal ou documentaire télévisé) …* ». (CNESCO, 2019). Le concept de translittératie tarde à se traduire en programme scolaire malgré de timides tentatives telles que le code dès la primaire. L'enjeu n'est pas seulement de former le public scolaire, mais en premier le personnel de l'Éducation nationale. De plus, assez peu est fait sur l'optimisation du rôle des bibliothèques et autres formes d'accès à la connaissance numérique. D'autre part, comme le précise la définition de l'Unesco citée, l'enjeu de la maîtrise de l'information n'est pas limité à la classe d'âge scolaire, mais s'inscrit clairement tout au long de la vie. Il est question d'autres enjeux de société tels que l'employabilité des seniors dans un environnement de travail de plus en plus numérique. Sur ce sujet des initiatives encore peu connues sont lancées par le gouvernement telles que la Grande École du numérique, groupe d'intérêt public lancé en 2015 chargé de « *diffuser ses formations partout sur le territoire en plus de ce qui va être fait dans le cadre de l'enseignement* » au moyen d'une labellisation de formations aux numériques au travers d'un réseau rassemblant : « *les ministères impliqués et leurs opérateurs, ainsi qu'un panel sélectionné et restreint d'acteurs privés en qualité de membres fondateurs de la structure.* » (Grande école du numérique, 2015). Ce type de partenariat public-privé avec des acteurs du numérique pose toutefois question en termes de neutralité, comme le partenariat entre

l'Education nationale et Microsoft pour développer le plan du numérique à l'école (Bancaud, 2016).

L'EMI est clairement un facteur de développement individuel et donc par extension est facteur de développement collectif, sociétal. Le fait que dans les 8 pays européens les plus développés, les individus âgés entre 18-29 ans vont avoir deux fois plus recours à l'internet pour se maintenir informés plutôt qu'à des médias traditionnels (Silver, 2018) est clairement un indicateur de l'impact de l'internet sur l'avenir d'une société. Cependant, le rôle de l'internet dans ce développement est dual, représentant autant d'opportunité que de dangers. Si un individu peut être éduqué, formé à une maîtrise de l'information alliant compétence technique et esprit critique, la nature des contenus auxquels il a accès relève d'un autre débat, celui de la législation nationale. Un individu lettré numérique doit également être un citoyen numérique, c'est-à-dire un défenseur des valeurs de la démocratie face aux attaques que subit celle-ci au travers de l'internet.

9.3. Maîtrise de l'information et sécurité des démocraties

En France, en 2015, le triptyque maîtrise de l'information, citoyenneté et univers numérique, malgré le rattachement à des valeurs citoyennes et démocratiques s'inscrit sans équivoque dans un contexte sécuritaire : « *À la suite des attentats de janvier 2015, l'éducation aux médias et à l'information a été renforcée, avec pour objectifs l'éducation à la citoyenneté et la transmission, à l'École, d'une culture de la presse et de la liberté d'expression. Les démarches éducatives visant à permettre aux élèves de comprendre et d'apprécier les représentations et les messages issus de différents médias, et en particulier de l'Internet, seront développées et encouragées. »* (Eduscol, 2015.). Le rapport au contexte sécuritaire est rappelé au travers de la prise en compte de l'EMI dans la lutte contre la radicalisation violente en milieu scolaire (Eduscol, 2019).

Ce lien entre EMI et sécurité est une vision gouvernementale et pas seulement du ministère de l'Éducation. Ainsi le ministère de la Culture lance en mai 2019 un appel à projets portant sur l'EMI dont l'une des quatre priorités est de : « *lutter contre les contenus haineux et déconstruire les théories complotistes dont la massification de la diffusion en ligne, notamment sur les réseaux sociaux, constitue un défi croissant pour notre société et notre démocratie* » (Ministère de la Culture, 2019). Cela montre que le but dépasse l'épanouissement individuel ou l'accomplissement intellectuel individuel. Le besoin en éducation, et enseignements aux médias et à l'information doit être à la hauteur de la menace que fait peser l'internet sur la démocratie et la sécurité de la société dans sa structure et son ensemble. Au niveau de la société, le rôle de l'information et des médias, leur influence sur les sociétés et la promotion de la démocratie est l'objet d'un champ d'études richement documenté (Curran et Hesmondhalgh, 2019 ; Mughan et Gunther, 2000 ; Lichtenberg, 1990).

Il est important de considérer qu'aujourd'hui l'individu a besoin de cette *maîtrise de l'information*, au sens global, car il se trouve à la fois dans un environnement informationnel non neutre, celui des médias traditionnels et numériques, et dans un environnement technique non neutre, celui d'internet. La non-neutralité de ces environnements se perçoit tant dans les définitions des concepts, toujours associés au concept de démocratie, que dans les cursus scolaires qui leur sont consacrés. Selon le Center for Media Literacy : « *L'éducation aux médias permet de mieux comprendre le rôle des médias dans la société ainsi que les compétences*

essentielles en matière d'enquête et d'expression de soi nécessaires aux citoyens d'une démocratie. » (Center for Media Litteracy, 2019).

Le lien entre éducation aux médias et démocratie est parfaitement décrit par Frédéric Lambert au cours de son intervention lors du Deuxième congrès européen de l'éducation aux médias en 2009 : « *Le jour où nos engagements politiques ne prendront plus en compte l'éducation aux médias comme faisant partie intégrale de cette culture de la démocratie, nous quitterons l'aventure de notre liberté chaque jour remise en question.* » (Lambert, 2009). La Commission Knight sur les besoins en information des communautés dans une démocratie estime que : « *Les personnes ont besoin d'informations pertinentes et crédibles pour être libres et autonomes.* » (Aspen Institute, 2019). Pour cela les universités jouent un rôle central selon Richard Howell, pour qui : « *Les médias, l'éducation et la démocratie sont indissociables, car une citoyenneté éduquée est essentielle au bon fonctionnement de la démocratie. Étant donné le rôle central des médias dans la démocratie, les médias ont non seulement l'obligation d'éduquer la citoyenneté, mais les universités doivent aussi éduquer la citoyenneté à propos des médias. Sans cette éducation, la démocratie elle-même est menacée.* (Howells, 2001). Ce rapport de l'individu aux médias, aux informations et donc à la démocratie est bousculé par les nouvelles technologies de l'information et de la communication, les nouveaux médias, plus globalement par l'internet. Le rôle d'internet et de l'éducation au numérique est explicitement mentionné dans le compte-rendu de la trente-deuxième session du Conseil des droits de l'homme de juin 2016 où celui-ci :

> *« 2. Reconnaît dans le caractère mondial et ouvert d'Internet un facteur déterminant pour accélérer le progrès vers le développement sous ses diverses formes, notamment pour atteindre les objectifs de développement durable ;*
>
> *4. Affirme qu'une éducation de qualité joue un rôle décisif dans le développement, et invite donc tous les États à promouvoir l'alphabétisme numérique et à favoriser l'accès à l'information sur Internet, qui peut être un outil important pour améliorer la promotion du droit à l'éducation* ; » (ONU, 2016).

La promotion d'internet comme outil démocratique vient de sa capacité à faire circuler l'information. Selon le rapporteur spécial de l'ONU Frank La Rue : « *Internet est l'un des instruments les plus puissants du XXIe siècle pour accroître la transparence dans la conduite des puissants, l'accès à l'information et pour faciliter la participation active des citoyens à la construction de sociétés démocratiques.* » (ONU, 2011).

Si l'internet est vu comme un facteur positif dans le développement de sociétés démocratiques, la libre circulation de l'information n'en demeure pas moins une source de grands dangers notamment auprès d'une population non éduquée, non lettrée numérique, et donc par extension une menace à la démocratie qu'elle est censée promouvoir.

Ce revers de la médaille s'exprime sous la forme de deux grandes menaces aux sociétés démocratiques : la haine en ligne et la désinformation ainsi que leurs variantes et conséquences.

- L'incitation à la haine est définie comme : « *tout comportement incitant publiquement à la violence ou à la haine dirigée contre un groupe de personnes ou un membre d'un tel groupe, défini par référence à la race, la couleur, la religion, l'ascendance ou l'origine nationale ou ethnique.* (Commission Européenne, 2008).
- La désinformation est définie comme : « *les informations dont on peut vérifier qu'elles sont fausses ou trompeuses, qui sont créées, présentées et diffusées dans un but lucratif ou dans l'intention délibérée de tromper le public et qui sont susceptibles de causer un préjudice public. Par préjudice public on entend les menaces aux processus politiques et d'élaboration des politiques démocratiques et aux biens publics, tels que la protection de la santé des citoyens de l'Union, l'environnement ou la sécurité.* » (Commission Européenne, 2018.)

Depuis 2016, l'Union européenne tend à voir l'internet pour ce qu'il est réellement, une opportunité autant qu'une menace en fonction des objectifs qu'il sert. Dans son rapport sur la communication stratégique de l'Union visant à contrer la propagande dirigée contre elle par des tiers, le parlement européen nomme spécifiquement la Russie comme fournisseur de désinformation : « *le Kremlin a intensifié sa confrontation avec l'Union* […] *; que le Kremlin a intensifié sa guerre de propagande, la Russie jouant un rôle plus actif dans l'environnement médiatique européen, afin de créer dans l'opinion publique européenne un soutien politique en faveur de l'action russe et de nuire à la cohérence de la politique étrangère de l'Union* » et l'État Islamique comme incitant à la haine : « *EIIL/Daech, Al-Qaïda et de nombreux autres groupes terroristes islamistes violents utilisent systématiquement des stratégies de communication et de propagande directe à la fois en ligne et hors ligne dans le cadre de la justification de leurs actions contre l'Union européenne et ses États membres et contre les valeurs européennes, ainsi que pour accélérer le recrutement de jeunes européens* » (Parlement Européen, 2016).

Pour la Commission européenne : « *les nouvelles technologies peuvent être utilisées, notamment par l'intermédiaire des médias sociaux, comme vecteur de désinformation à une*

échelle jamais atteinte, avec une rapidité et une précision de ciblage sans précédent. […] *Une série d'acteurs nationaux et étrangers ont largement recours à des campagnes massives de désinformation en ligne pour semer la méfiance et créer des tensions sociétales, ce qui peut avoir de graves conséquences pour notre sécurité. En outre, les campagnes de désinformation menées par des pays tiers peuvent faire partie de menaces hybrides à la sécurité intérieure, y compris dans le cadre des processus électoraux, en particulier lorsqu'elles s'accompagnent de cyberattaques.* ». (Commission Européenne, Op.cit.).

Pour lutter contre la désinformation, elle préconise des solutions basées essentiellement sur les capacités et compétences des citoyens à évaluer le contenu qui leur est accessible, favoriser la diversité de l'information et le journalisme de qualité, mettre en œuvre des signaleurs de confiance dans la qualité de l'information, et enfin se reposer sur l'éducation aux médias au travers de coopération entre toutes les parties prenantes : utilisateurs, pouvoirs publics, diffuseurs, médias, etc.

Cette approche inclusive de toutes les parties prenantes à l'internet est en phase avec les « *Principes globaux de La Haye sur la responsabilité à l'ère numérique* » édictés par l'Institut pour la responsabilité à l'ère numérique (I4ADA, 2018), association à but non lucratif multipartite se donnant pour mission d'étudier le partage de responsabilité sur l'internet. Cependant, la notion de responsabilité, de l'anglais accountability, entend une responsabilité devant la loi en cas d'infraction. Ainsi le Code de conduite sur la réponse aux discours illégaux de haine en ligne de 2016 lancé en partenariat avec des entreprises de l'internet (Facebook, Twitter, Youtube, Microsoft) renforce encore la notion de responsabilité des diffuseurs, ce qui va à l'encontre de leur position de neutralité. Ce code estime que les entreprises de l'internet : « *partagent, avec d'autres plateformes et entreprises de médias sociaux, une responsabilité collective et une fierté de promouvoir et de faciliter la liberté d'expression dans le monde en ligne* ». (Commission Européenne, 2016).

Il paraît évident que ce code de conduite va être âprement disputé devant les tribunaux par l'ensemble des signataires car les entreprises de l'internet refusent d'endosser la responsabilité des contenus qu'elles diffusent comme le mentionne l'Internet Association, principale structure de lobbying des entreprises de l'internet : « *Internet a fleuri en partie parce que les plates-formes Internet permettent aux utilisateurs de publier et de partager des informations sans craindre que ces plateformes soient tenues pour responsables du contenu de tiers.* » (Internet Association, 2019). À l'échelle nationale, la transcription dans la loi des principes européens ne se fait pas sans débat. En 2017, l'Allemagne est le premier pays européen à mettre en place

une loi portant sur la lutte contre le contenu haineux, le Network Enforcement Act (NetzDG). Elle a procédé à la première condamnation d'une entreprise d'internet (Facebook) en 2019 pour un montant de 2 millions d'euros pour avoir failli à son obligation de transparence sur la manière dont elle gérait les plaintes reçues au sujet de contenu haineux. (apnews.com, 2019). En France, la proposition de loi AVIA, basée sur la loi allemande, met en place des procédures pour lutter contre les discours de haine en 2019 qui prévoit, si elle est adoptée par le sénat que : « *Dans les mêmes conditions, l'autorité administrative peut également demander à tout moteur de recherche ou tout annuaire de faire cesser le référencement des adresses électroniques donnant accès à ces contenus. Lorsqu'il n'est pas procédé au blocage ou au déréférencement des contenus en application des deux premiers alinéas, l'autorité judiciaire peut être saisie, en référé ou sur requête, pour ordonner toute mesure destinée à faire cesser l'accès à ces contenus.* (Assemblée Nationale, 2019). Dans la mise en œuvre de ces lois, en plus du lobby des entreprises de l'internet, les législateurs ont été accusés de censure par les associations de défenses des droits des utilisateurs de l'internet : « *En l'espèce, imposer un délai de 24h pour retirer un contenu manifestement illicite est susceptible de provoquer d'importantes restrictions de libertés, tel que le sur-blocage de propos licites ou le dévoiement de la mesure à des fins de censure politique*. (Quadrature du net, 2019).

La régulation du contenu par les gouvernements est un facteur de perte de maîtrise de l'information par les citoyens, même si la législation est mise en place avec les meilleures intentions notamment celle de protéger les citoyens de contenus dangereux pour la démocratie. Cette lutte nationale pour protéger ses citoyens s'inscrit dans une lutte globale pour le contrôle des utilisateurs de l'internet. En plus d'objectifs sécuritaires, des objectifs économiques sont également en jeu et ils ont un impact sur l'accès à l'information et donc sa maîtrise par un individu, un citoyen, relégué au rang de simple utilisateur.

9.4. Maîtrise de l'information et régulation de l'internet

Quand bien même un citoyen dispose d'une éducation, d'une formation, et d'une appétence pour l'information disponible sur l'internet, il n'en est pas maître pour autant. Outre les attaques délibérées pour falsifier l'information disponible et pour inciter à la haine et la polarisation des sociétés, qu'elles soient menées par des États, des groupes ou des individus, le citoyen lettré numérique reste redevable d'une lutte dépassant le contenu, mais portant sur la gouvernance même du réseau international.

Deux facteurs de perte de maîtrise de l'information sont particulièrement inquiétants : l'un est la maîtrise des infrastructures de l'internet, soit sa gouvernance, et l'autre est la neutralité du web, deux thèmes qui sont sources de débats complexes entre États, organisations gouvernementales internationales, organisations non gouvernementales, entreprises et citoyens. D'après un rapport du Groupe de haut niveau sur la coopération numérique du Secrétaire général des Nations Unies publié en 2019, nous sommes dans une ère d'interdépendance numérique qui requiert une coopération accrue : « *Il a été largement admis qu'une coopération améliorée est nécessaire, qu'une telle coopération devra revêtir de multiples formes et que les gouvernements, le secteur privé et la société civile devront trouver de nouveaux moyens de travailler ensemble pour tracer efficacement la voie entre les extrêmes que sont la réglementation excessive et le laissez-faire complet.* » (ONU, 2019) Aucun pays ne dispose d'une infrastructure d'internet 100% nationale, pas même la Chine ou la Russie malgré leur volonté d'avoir un réseau national connecté à l'internet (via des passerelles supervisées). Tous les pays sont interdépendants que cela soit pour l'accès à des technologies servant à l'infrastructure ou pour des accès au maillage global (dorsales d'accès, dit « backbone »), d'où le besoin d'une gouvernance partagée. La neutralité d'internet, quant à elle, est le principe selon lequel les fournisseurs de services à l'internet et les gouvernements doivent traiter toutes les données sur l'internet de la même manière, sans discrimination ni tarification différenciée par utilisateur, contenu, site, plateforme, application, type d'équipement connecté ou mode de communication (Singh, 2017).

La notion de contrôle des infrastructures et du contenu de l'internet dépend des interlocuteurs concernés, ces derniers sont très différents et doivent répondre d'une part à des enjeux économiques se comptant en centaines de milliards d'euros et d'autre part à des enjeux de sécurité fragilisant les fondements de société tels que décrits précédemment. Malgré cette

interdépendance évidente, une des sources de complexité est l'absence de territorialité de l'internet, et donc l'impossibilité d'y appliquer une législation spécifique : « *Les espaces Internet ne sont ni territoriaux ni supra-territoriaux, mais une combinaison et une interaction des deux. En conséquence, les aspects territoriaux et supra-territoriaux d'Internet ne peuvent être dissociés et mesurés séparément. Au contraire, la géographie du cyberespace comprend toujours des interconnexions inextricables de conditions territoriales et supra-territoriales* » (Scholte, 2018). Ce principe de *transcalarité* tel que défini par Scholte, c'est-à-dire cette prise en compte nécessairement simultanée de toutes les échelles géographiques du local à l'international se retrouve au niveau de la gouvernance avec la prise en compte d'associations à but non lucratif, d'organisations intergouvernementales, de gouvernements nationaux, d'entreprises multinationales, etc.

L'Unesco définit la gouvernance de l'internet de la façon suivante : « *La gouvernance de l'internet est le fruit d'un développement et d'une application complémentaire de la part des gouvernements, du secteur privé, de la société civile et de la communauté technique qui, dans leurs rôles respectifs, partagent des principes, des normes, des règles, des processus de prise de décision et des activités définissant l'évolution et l'usage de l'Internet.* » (Unesco, 2013 b).

Ci-dessous, une illustration uniquement des entités internationales concernées par la gouvernance de l'internet :

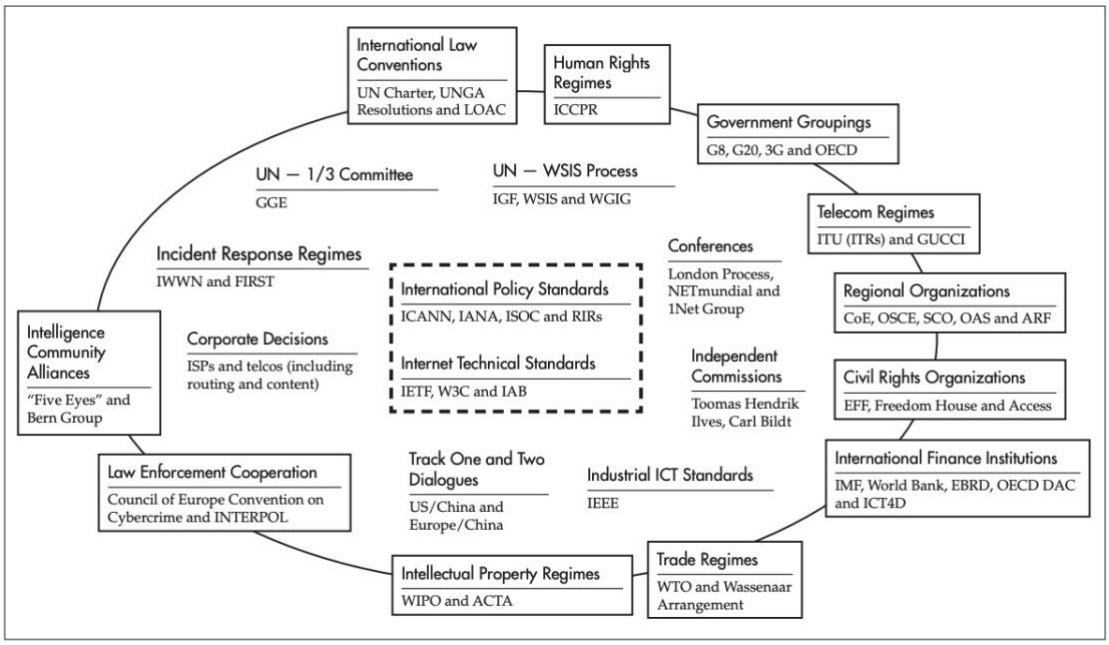


Figure 69 : Le système du régime de gestion des activités cybernétiques mondiales, (Nye, 2014)

Il s'agit de faire s'entendre une grande disparité d'interlocuteurs aux intérêts souvent divergents et aux moyens très différents. Parmi les entités représentées se trouvent : les gouvernements et organisations supranationales qui régulent l'internet à l'intérieur de leur juridiction et contribuent à influer sur la gouvernance globale ; les associations de citoyens qui se chargent de défendre les utilisateurs ; et une accumulation d'acteurs grandissant avec l'évolution de l'internet. Au début l'internet était régulé par des entités administratives et/ou techniques militaires puis civiles, publiques puis privées, toutes américaines. A la création d'internet ARPANET (1970) Internet Engineering Task Force (1986), Internet Assigned Numbers Authority (1988), Internet Society (1992), Web consortium (1994), Internet Corporation for assigned names and numbers (1998), *etc.* Ces organisations privées américaines à but non lucratif ont également évolué avec le temps, tant dans le domaine technique que dans le domaine administratif : *« Ce sont maintenant des organisations plus complexes et des organisations plus grandes qu'auparavant. Cette évolution a entraîné une modification de la manière dont ils envisagent leur mandat et croient en ce qu'ils pensent que leur place dans le monde devrait être. Cet ensemble d'organisations a grandi, nous sommes passés de quatre nœuds de la précédente incarnation d'Internet en 1969 à des millions et des millions maintenant, les attentes à l'égard de ces organisations ont changé, tant à l'intérieur qu'à l'extérieur. » (Sadowsky, 2011).* Malgré leur évolution du secteur gouvernemental vers le secteur privé, celle-ci est restée dans le contexte territorial et législatif des États-Unis même si l'influence de ces derniers est en décroissance, l'intérêt des entreprises citées pouvant diverger avec celui de l'État américain.

Au fur et à mesure que l'internet se développait, de puissants acteurs ont voulu avoir leur mot à dire sur la circulation des informations sur le réseau. Il y a tout d'abord eu les opérateurs téléphoniques responsables des infrastructures techniques des dorsales du réseau, puis les fournisseurs d'accès à l'internet et enfin les fournisseurs de services sur l'internet et plus particulièrement sur le web. Ainsi, le développement des technologies du web et leur intégration dans la vie économique sont allés croissant et ce faisant représente aujourd'hui des implications financières qu'aucune autre technologie n'avait atteint auparavant. En 2015, selon une estimation de la Conférence des Nations Unies sur le Commerce et le Développement, le total des ventes du e-commerce représentait $25.3 billions (milliards de milliards) de dollars. De tels montants expliquent la volonté des nouveaux acteurs économiques de faire entendre leur position sur la façon dont l'internet est dirigé alors que numériquement ils ne représentent qu'une minorité d'acteurs dans la gouvernance de l'internet, voir figure 70.

Figure 70 : Taxonomie des parties prenantes à la gouvernance de l'internet (Kalogiros, 2012)

Si la règle de gouvernance d'internet repose sur le multipartisme, l'ouverture et la coopération, les débats se règlent *in fine* dans les tribunaux et les amendes se comptent en millions voire en milliards en fonction de l'échelle (internationale ou nationale).

Ces batailles juridiques peuvent concerner des désaccords entre deux acteurs de l'internet comme l'illustre l'affrontement entre des fournisseurs d'accès à l'internet (FAI) (tels qu'Orange, Free, *etc.*) et des fournisseurs de contenu (Youtube, Dailymotion, etc.) ou de service (Skype, Messenger, *etc.*). Dans ce cas, les FAI pour des raisons strictement économiques, limitent les services et donc la circulation de l'information (Fradin, 2012 ; Slate 2013). La notion de maîtrise de l'information par les utilisateurs de l'internet se fait plus ressentir quand le contenu disputé concerne une chaîne d'information. En 2019, de simples enjeux de partage de revenus ont bloqué la diffusion de la chaîne d'information BFMTV via les réseaux des fournisseurs d'accès à internet (FAI) Orange et Free. Alors que les opérateurs des chaînes estiment qu'ils contribuent à l'attractivité des FAI et doivent toucher une part de l'abonnement des services d'accès à l'internet, ces derniers considèrent qu'ils diffusent gratuitement le contenu de ces chaînes et n'ont rien à redistribuer. Le résultat de cet affrontement est immédiat pour l'utilisateur des FAI : une perte d'accès à l'information, et immédiat pour la chaîne

d'information : une perte d'audience (France Info, 2019). En France, cette bataille pour les revenus issus des abonnements des utilisateurs de l'internet fait suite à de nombreux autres conflits avec des chaînes généralistes telles que M6 ou TF1 où les montants sont de l'ordre de 20 millions d'euros de redevance annuelle réclamés par TF1 (Europe1, 2018). Ces passes d'armes contractuelles et parfois juridiques relèvent strictement du droit privé sur lequel l'État n'a pas à intervenir. Cependant l'utilisateur in fine n'est pas en mesure de maîtriser le contenu que voudra bien lui diffuser le FAI.

Ces batailles prennent une autre dimension lorsqu'elles impliquent des multinationales et des gouvernements. Pour autant il faut raison garder. Les multinationales en question sont toutes américaines, comme le sont les autorités de régulation de l'internet. Il s'agit de Google, Amazon, Apple, Facebook, et Microsoft qui ont à elles cinq une évaluation à 4,1 billions (milliards de milliards) de dollars (Chen, 2018). Cette puissance financière se traduit en capacité d'influence sur l'internet, même si celle-ci est de plus en plus contestée par les gouvernements et organisations intergouvernementales : Google *vs* l'Union européenne (1,49 milliard d'euros d'amende pour le géant américain pour abus de position dominante).

Malgré ces affrontements juridiques, toutes les parties prenantes ont un intérêt à limiter l'impact sur l'infrastructure globale d'internet. Aucune partie n'a le moindre intérêt d'un repli sur soi, d'une fédéralisation de l'internet en une interconnexion globale d'instances locales.

Cette nécessaire co-gestion explique la création d'une nouvelle instance de concertation en 2006 : le Forum sur la gouvernance de l'Internet (IGF) en tant qu'espace neutre de débat sous l'égide de l'ONU créé en 2006 : « *il sert à rassembler des membres des diverses parties prenantes sur un pied d'égalité lors de discussions sur des questions de politique publique relatives à Internet. Bien qu'il n'y ait pas de résultat négocié, l'IGF informe et inspire les personnes disposant d'un pouvoir décisionnel dans les secteurs public et privé.* » (Internet Governance Forum, 2019).

La gouvernance d'internet, complexe à définir, est en perpétuelle évolution compte tenu de l'évolution même de la technologie. Aucun modèle de gouvernance définitif n'est visible à un avenir proche : « *Il est peu probable qu'il y ait un régime global unique pour le cyberespace dans un avenir proche. Une forte fragmentation existe actuellement et devrait persister. L'évolution du complexe de régime actuel, qui se situe à mi-chemin entre une seule structure juridique cohérente et une fragmentation complète des structures normatives, est plus probable.* » (Nye, *op. cit.*). Il est aujourd'hui plus question de définir un mode opératoire qu'un cadre législatif commun : « *le fait que les principaux acteurs de la gouvernance de l'Internet*

souscrivent à diverses conceptions de la légitimité procédurale contribue à expliquer la tension croissante dans ce domaine et suggère également que les acteurs devraient tenter de forger un modus vivendi procédural avant de tenter de résoudre des problèmes de fond. » (Raymond et DeNardis, 2015).

Au-delà des enjeux de la gouvernance globale de l'internet, le sujet de la neutralité de celui-ci, (ou plutôt de son impossible neutralité celle-ci étant chaque jour davantage menacée) est également un enjeu de la maîtrise de l'information en tant que question majeure à la fois éducative et politique. La neutralité d'internet dans son ensemble a un impact potentiel considérable sur les processus démocratiques ou les influences possibles à l'échelle d'un pays, d'une population, d'une région. Pour mesurer l'impact de la neutralité de contenu, Serge Abiteboul prend pour exemple la position ultra-dominante du moteur de recherche de Google qui représente 90% des recherches effectuées sur le web au niveau mondial : « *Quand une entreprise maîtrise la recherche sur le Web, les réseaux sociaux, les magasins d'applications, les objets connectés ... utilisés par une énorme partie de la population, elle a la possibilité de contrôler les choix de centaines de millions, voire de milliards d'individus. Sa responsabilité est immense. Il paraît normal de lui demander d'être neutre dans son hébergement et dans ses recommandations de services de tiers*. ». (Abiteboul, 2018). Malgré des efforts continus sur le sujet, la neutralité de l'internet est très complexe à réguler, car elle dépend de cadres législatifs nationaux s'inscrivant dans des accords internationaux. De plus, elle dépend d'une multitude d'intervenants privés multinationaux qu'ils s'agissent de fournisseurs d'accès à l'internet (par exemple Orange), de fournisseurs de services (par exemple Facebook) ou de fournisseurs de technologie d'infrastructure (par exemple Huawei). La neutralité d'internet fait l'objet de multiples débats sur des sujets sensibles et clivants comme l'affrontement entre les partisans du contrôle de sécurité pour éviter la diffusion de contenus illicites et les partisans du respect de la vie privée. Dans ce débat sans fin, ayant lieu entre les gouvernements et les associations de défense de droits des utilisateurs, les fournisseurs d'accès et de technologie souhaiteraient rester neutres. Tant qu'ils n'ont pas connaissance du contenu, ils ne peuvent endosser la responsabilité de leur diffusion, mais ils sont appelés par les États à contribuer à la sécurité nationale en divulguant des informations si nécessaire. Toujours est-il qu'une législation se met en place, partout dans le monde, même au sein de démocraties comme celles de l'Union européenne, qui tendent à privilégier le caractère sécuritaire : « *La réglementation d'Internet, qui est en train de se mettre en place rapidement, est conduite - sans aucun doute - par les politiciens européens pour des raisons de sécurité publique. Ils érigent des barrières à l'entrée avec la connivence des acteurs historiques, avec des conséquences potentiellement énormes pour la liberté*

d'expression, pour la libre concurrence et pour l'expression individuelle. C'est peut-être la bonne option pour une politique Internet plus sûre (pour empêcher d'exposer les enfants à un contenu illégal et / ou offensant et pour lutter contre les activités criminelles graves), bien que cela signale un changement brutal de l'Internet ouvert. » (Marsden, 2017). Les sujets de la gouvernance et de la neutralité ont un impact sur la nature de l'information à laquelle un utilisateur de l'internet a accès. Ces débats ne lui sont pas accessibles car ils sont gérés à très haut niveau, et pour cela il ne peut pas dire qu'il maîtrise le contenu auquel il a accès.

9.5. Conclusion

La maîtrise de l'information se définit de façon différente que l'on se place du point de vue de l'individu, du citoyen ou de l'utilisateur d'internet. Le rôle d'internet dans la façon dont nous avons accès à l'information va croissant. À titre individuel, cela requiert une capacité technique et cognitive, un ensemble de capacités et de compétences individuelles afin d'être en mesure d'utiliser et non pas de subir notre environnement informationnel. Cet ensemble appelé translittératie est désormais indispensable au développement de tout individu au point d'être reconnu comme droit fondamental par les Nations Unies. Il est du ressort de chaque État de mettre en œuvre des politiques éducatives, des enseignements permettant, à tout individu et à tout âge, d'acquérir cette translittératie.

Chaque état démocratique à un intérêt réel à le faire. Les individus lettrés numériques étant des citoyens numériques, le transfert des valeurs de la société se font désormais également via l'information disponible sur l'internet. Cet impact de l'information transmise en fait un enjeu de pouvoir, d'influence, et un moyen d'attaque d'une société démocratique, d'une organisation intergouvernementale. Le citoyen doit donc renoncer à une part de sa maîtrise de l'information au profit d'une sécurité de l'information garantie par l'État. Ce dernier, au nom des intérêts supérieurs de la Nation, doit protéger ses citoyens des tentatives de déstabilisation que sont la désinformation et les discours de haine en provenance de criminels, voire d'ennemis.

Comme chaque individu est citoyen, chaque citoyen (ou presque) est utilisateur de l'internet. Ce réseau ne permet pas une véritable maîtrise de l'information à ses utilisateurs. Sa gouvernance intrinsèque et sa neutralité sont régulièrement remises en question. Elles font l'objet de luttes acharnées entre entités gouvernementales en compétition l'une avec l'autre, entités privées elles-mêmes concurrentes, une forme de *bellum omnium contra omnes* : la guerre de tous contre tous, au détriment de l'intérêt du collectif, du citoyen, de l'utilisateur.

La remise en question de la maîtrise du contenu de l'internet ne remet pas en question la nécessité de la mise en œuvre de politique de translittératie. Au contraire elle les rend plus indispensables encore. La protection du citoyen du contenu préjudiciable, à distinguer du contenu illicite, et la détection et neutralisation de la désinformation interne et externe doivent se traduire par la mise en capacité des forces de l'ordre et des forces armées. Or, à ce jour, nous ne sommes qu'aux prémices d'une certaine forme de législation. La mise en œuvre de systèmes de détection tels que décrits dans nos travaux reste à faire.

Conclusion de la troisième partie

Comme nous l'avons indiqué dans la partie précédente, la guerre hybride s'inscrit à la fois dans une permanence du conflit où tout moyen de pression sur l'adversaire est légitime. Nous avons expliqué comment les services de renseignement seraient en mesure d'agir dans cet environnement. Cependant, ils ne sont pas les seules parties prenantes. Un des moyens de pression consiste à saper la confiance des citoyens dans leurs dirigeants, à amplifier les clivages de la société, à opérer sur l'opinion publique. Les opérations menées sont de natures variées, et certaines ont spécifiquement lieu sur les réseaux sociaux. Les opérations d'influence sur des processus électoraux sont assez fréquentes, mais la diffusion de fake news, elle, est quasi quotidienne. Il existe plusieurs méthodes pour se défendre allant de la diffusion de contre-discours jusqu'à la fermeture de serveurs relayant ces opérations. Cependant, pour se défendre il faut être en mesure de détecter l'attaque et d'en comprendre le mécanisme. A cette fin nous avons suivi deux évènements pour illustrer notre méthodologie d'analyse, les élections européennes en France de mai 2019 et une fake news portant sur la Syrie. Si les deux opérations n'ont pas eu d'impact sur la société, elles permettent d'expliquer le but, la méthode et l'impact potentiel de ces opérations. L'efficacité des plateformes analytiques appuyées par l'intelligence artificielle dépasse le cadre strict militaire. Ces mêmes plateformes peuvent également contribuer à sécuriser la société de l'intérieur en étant déployées auprès des forces de l'ordre. Si nous nous inscrivons contre le concept de police prédictive, nous revendiquons la nécessité de mettre en œuvre une police guidée par le renseignement. Nous avons montré comment les principes du renseignement tels que les conçoivent les forces armées, en tant que fonction éclairant la planification et la conduite des opérations, sont parfaitement transposables au domaine policier. Il est impensable pour une unité militaire d'opérer sans connaissance du terrain, de l'adversaire et des autres parties prenantes, il devrait en être de même pour les unités de police. La police guidée par le renseignement est une police qui intègre les fonctions de renseignement à tous les niveaux opératifs et qui ne réserve pas cette capacité exclusivement à une direction générale qui deviendrait de ce fait un goulot d'étranglement.

La sécurité et la défense de la société reposent sur des forces armées et des forces de l'ordre adaptées à l'environnement physique et numérique sur lesquels se déroulent les combats modernes, mais pas seulement. Une société résiliente repose sur la maîtrise collective de l'information. Cette maitrise de l'information peut signifier différentes choses pour les chercheurs, mais elle doit se traduire dans les faits par des citoyens lettrés numériques à même

de ne pas se laisser influencer par des opérations adverses. Ces citoyens ne pourront maîtriser leur environnement informationnel, composé essentiellement de médias et de contenu sur l'internet, que s'il y est formé Les politiques d'éducation aux médias et à l'information doivent se mettre à la hauteur des enjeux auxquels fait face la société. Ceci est d'autant plus important que l'internet est l'objet de luttes permanentes pour son contrôle ou le maintien d'une absence de contrôle. Si la défense d'une gouvernance partagée et d'une volonté de neutralité doit guider les négociations, compte tenu des opérations de guerres hybrides et de l'utilisation de l'internet à des fins criminelles, une capacité de régulation légitime et sous contrôle citoyen doit également être mise en œuvre.

Conclusion générale

Notre expérience de 18 années au sein du ministère de la Défense est à l'origine de nos travaux. Nos diverses affectations, en France comme à l'étranger, en tant que capteur ou analyste, ont un fil conducteur, une mission : comprendre et anticiper les évènements. L'objet de cette mission n'est pas seulement d'être en mesure de chercher et de recueillir la donnée, mais aussi d'être en mesure de l'exploiter. En effet, il n'y a rien de plus frustrant pour un agent que de produire un renseignement incomplet alors que l'information était quelque part disponible. Une partie de notre expérience a tourné autour de l'exploitation de l'internet à des fins de renseignement, pour faire ce qui s'appelle du renseignement de sources ouvertes. Cette forme de renseignement est rarement l'objet de recherche académique en France, même si le renseignement en général n'est beaucoup mieux représenté. Or cette forme de renseignement qui est la plus en lien avec la société civile mérite une recherche spécifique. Il n'est pas question d'imagerie satellite ou d'interception de communication. Il s'agit, la plupart du temps, de recueillir, d'exploiter et d'analyser ce qui se dit sur l'internet.

Au moment où démarrait la crise ukrainienne, aucun analyste n'avait été en mesure de la prédire, ni même de la détecter. Véritable surprise stratégique, cette crise a rapidement été considérée comme l'archétype de la guerre hybride, au même titre que les Printemps Arabes qui ont été nommés « Twitter Revolutions ». C'est d'ailleurs un point commun entre ces crises et les crises des dix dernières années : le rôle des médias sociaux numériques, sans qu'ils soient prépondérants, leur présence au sein des conflits, sont manifestes. Creuset de toutes nos expériences et de nos questionnements, nos travaux ont eu pour objectif de répondre à quelques questions en vue d'éviter que la prochaine crise soit une surprise.

La première question à laquelle nous souhaitions répondre porte sur l'adaptation du renseignement de sources ouvertes aux conflits modernes. Comment prendre en compte les dynamiques d'un conflit social ? Quels sont les cadres et théories qui permettent d'anticiper les évolutions de potentielles « guerres de mouvements sociaux » et quel impact cela a sur le renseignement tel qu'il est pratiqué aujourd'hui ? Anticiper est-ce prédire ?

Une fois que l'on dispose d'un cadre théorique pour observer et comprendre un mouvement social, la seconde question porte sur le processus de création de renseignement. Comment mieux capitaliser sur les processus existants pour adapter la fonction aux conflits modernes ? Que peuvent apporter les méthodes d'exploitation analytique du « big data » à la

compréhension d'un conflit ? Enfin la dernière question revient sur le concept de guerre hybride et de son impact sur la société. A quoi faut-il s'attendre comme opération adverse ? Comment utiliser les pratiques du renseignement pour augmenter la sécurité des citoyens ? Comment rendre la société plus résiliente au moyen de la maîtrise de l'information ?

Nous avons cherché, au travers de nos travaux, à éprouver certaines hypothèses. La première était que les sciences humaines et sociales (SHS), en particulier les sciences de l'information et de la communication (SIC) étaient nécessaires à la compréhension des guerres de mouvements sociaux. Non seulement les théories du conflit sont utiles mais l'analyse du lien essentiel entre les conflits et l'évolution des moyens de communication, aujourd'hui les réseaux sociaux, doivent être intégrées au renseignement militaire dans de tels contextes.

La deuxième hypothèse était que ces conflits modernes, c'est-à-dire ces théâtres connectés où toute partie prenante active ou passive est un capteur, une source d'information potentielle, changent la façon de recueillir et d'exploiter l'information.

La troisième hypothèse était que les pratiques du renseignement militaire adaptées à l'internet et à la guerre hybride peuvent également contribuer à la sécurisation de la société, bien qu'elles ne suffisent pas. Pour augmenter la résilience de la société face aux nouvelles menaces, celle-ci doit avoir une maîtrise de l'information à plusieurs niveaux, comme des lignes de défense successives : au niveau de l'individu, au niveau de la société, au niveau de l'internet.

Nos résultats ont montré que la méthodologie du « protest event analysis » était parfaitement adaptée au renseignement et aux guerres de mouvements sociaux pour peu qu'elle soit adaptée à la nature des données disponibles aujourd'hui. Au sujet des données, celles générées par les utilisateurs de l'internet (user generated content), notamment celles diffusées via les réseaux sociaux sont essentielles. Ces données, leurs usages et leur traitement étant, entre autres, dans le champ de compétences des SIC, le renseignement a un double intérêt à développer ses relations avec le monde académique. Nous appelons donc à une évolution du cycle du renseignement pour une meilleure prise en compte des modes de communication de la société civile. Cette évolution doit se faire tant au niveau des concepts qui régissent le renseignement de sources ouvertes que des technologies mises en œuvre. L'internet n'est pas seulement un dépôt de données. Les technologies de haut niveau (et en constant progrès) utilisées sur cette infrastructure Internet doivent être intégrées et adaptées aux activités d'un service de renseignement. Cette adaptation devient urgente car les nouveaux conflits sont déjà en cours.

Comme nous l'avons expliqué, les occidentaux accusent, essentiellement les russes, de mener une « guerre hybride » permanente employant l'information comme moyen de destruction et

l'internet comme vecteur de diffusion. En contrepartie, les russes prennent très au sérieux le concept de « guerres des mouvements sociaux ». Ainsi le ministre russe de la Défense, Sergueï Choïgou, remarque que « *les problèmes socioéconomiques de certains pays servent de prétexte pour remplacer les gouvernements à orientation nationale par des régimes contrôlés depuis l'étranger. Ces régimes offrent à leurs clients un accès sans entrave aux ressources de ces pays.* » (Flintoff, 2014). Cette remarque vise clairement les occidentaux qu'il accuse de fomenter des troubles sociaux au nom de valeurs qui leur sont propres. Et on ne pourrait pas le lui reprocher lorsqu'on a étudié les principes de « démocratisation » tels qu'ils sont mis en œuvre par les Etats-Unis par exemple. Au vu de la pénétration de l'internet dans les sociétés son impact est immense et il est aisé de voir comment un pays est déstabilisé par un mouvement social si ce dernier tend vers un conflit violent, voire armé. Micah White, chercheur américain spécialisé dans l'activisme confirme qu'un : « *un tournant vers la guerre des mouvements sociaux pourrait constituer une réponse stratégique à la non-faisabilité de la confrontation directe, ou de la guerre classique, contre les grandes armées et les États dotés de l'arme nucléaire.* » (White, 2016).

Pour décrire le lieu où se déroule ce nouveau type de conflit nous avons défini le concept de théâtre d'opérations connecté (TOC). La crise ukrainienne s'est avérée un parfait exemple de ce type de théâtre. Ce TOC vient en complément du champ de bataille classique. Il en est l'émanation numérique. Ce n'est pas une simple transposition d'attaque et de défense d'infrastructure numérique intéressant seulement la cybersécurité. Il prend en compte le combat pour et par l'opinion publique, le combat sur la structure même de la société adverse. C'est pourquoi nous avons jugé utile de montrer comment se renseigner sur ces conflits au travers des réseaux sociaux et de l'exploitation analytique de leurs données. La combinaison des outils d'analyses statistiques avancées, d'analyses sémantiques et d'analyses de réseaux donnent la capacité d'anticiper les évolutions des conflits. Dans la très forte volumétrie et vélocité des informations circulant sur les réseaux sociaux, la méthodologie DETEVEN permet de focaliser l'attention de l'analyste sur les évènements, c'est-à-dire les faits marquants qui changent le cours de l'histoire. Cette méthodologie permettrait de mettre en œuvre des plateformes qui assisteraient et guideraient les analystes. Elles automatiseraient les tâches les plus répétitives et l'intelligence artificielle, ou plutôt le *machine learning* (apprentissage machine), en améliorerait constamment la pertinence. Une fois les évènements détectés, il est alors possible d'en comprendre les causes et conséquences afin d'élaborer des scénarios d'évolution probables priorisés par probabilité de survenue. Nous affirmons que pour cette phase d'analyse, la technologie ne suffit pas, elle n'est possible qu'avec l'appui des SHS et des SIC pour la cadrer.

Au-delà du théâtre d'opérations connecté, nous avons voulu démontrer l'intérêt d'une telle capacité sur le territoire national. En effet, ce dernier peut être la cible d'un adversaire pratiquant la guerre hybride ou la guerre de mouvements sociaux. Outre le terrain ukrainien décrit dans cette thèse, nous avons analysé deux situations réelles, celle de la surveillance d'une période électorale et celle de la diffusion d'une *fake news*. Nous en avons expliqué les principes et pratiques, puis nous avons démontré comment il était possible de les mettre sous surveillance au travers de la même plateforme utilisée par le renseignement militaire. Nous avons même illustré l'interculturalité du renseignement militaire et de la police guidée par le renseignement, l'*intelligence-led polcing*. Au travers de ces cas d'usage concrets nous avons voulu casser le mythe de la police prédictive par la mise en évidence des dangers liés à la conception des algorithmes, l'exploitation limitée des données et la difficile attribution de responsabilités. En opposition à cette police tournée vers la prédiction, nous appelons à une police guidée par le renseignement, de la même façon qu'une opération militaire se conduit. En revanche, un citoyen n'est pas un ennemi. C'est justement parce que ces plateformes de renseignement policier permettent une plus grande efficacité, une plus grande efficience et une plus grande transparence qu'elles doivent être mises en œuvre dans le cadre légal qui régit la police. D'une meilleure exploitation des données, on obtient un plus grand contrôle de celles-ci.

Enfin, nous avons voulu élargir nos travaux à la maîtrise de l'information. Si la société est une cible de la guerre hybride, les attaques se font au travers de ses citoyens. Une des façons d'opérer sur la société est d'atteindre son opinion publique, de créer des clivages, de faciliter la polarisation, voire de contribuer à la provocation d'un mouvement social. La fonction de renseignement de l'État doit être en mesure de détecter les prémices de ce type de situation, de détecter les évènements. Quant au citoyen, il doit être en mesure de maîtriser son environnement informationnel, de distinguer le vrai du faux, de repérer les mécanismes d'influence. Cette maîtrise de l'information à l'échelle individuelle ne peut s'obtenir que grâce à une montée en compétence et en capacité permettant l'acquisition d'une translittératie numérique. Il est donc du ressort de la société de mettre en œuvre une éducation aux médias et à l'information et la rendre disponible tout au long de la vie. Ces efforts éducatifs individuels et collectifs ne suffiront pas sans un engagement de tous les niveaux de la société particulièrement difficile, mais indispensable, concernant deux sujets majeurs qui conditionnent l'accès à l'information : la gouvernance d'internet et la neutralité du Web. Les enjeux sont colossaux si l'on considère l'aspect financier, mais ils vont bien au-delà de cela. Il est question ici d'être en mesure de jouer un rôle pour maintenir l'internet tel qu'il a été conçu, un formidable outil de développement de l'humanité et pas seulement un nouveau champ de bataille. Après une longue période sans

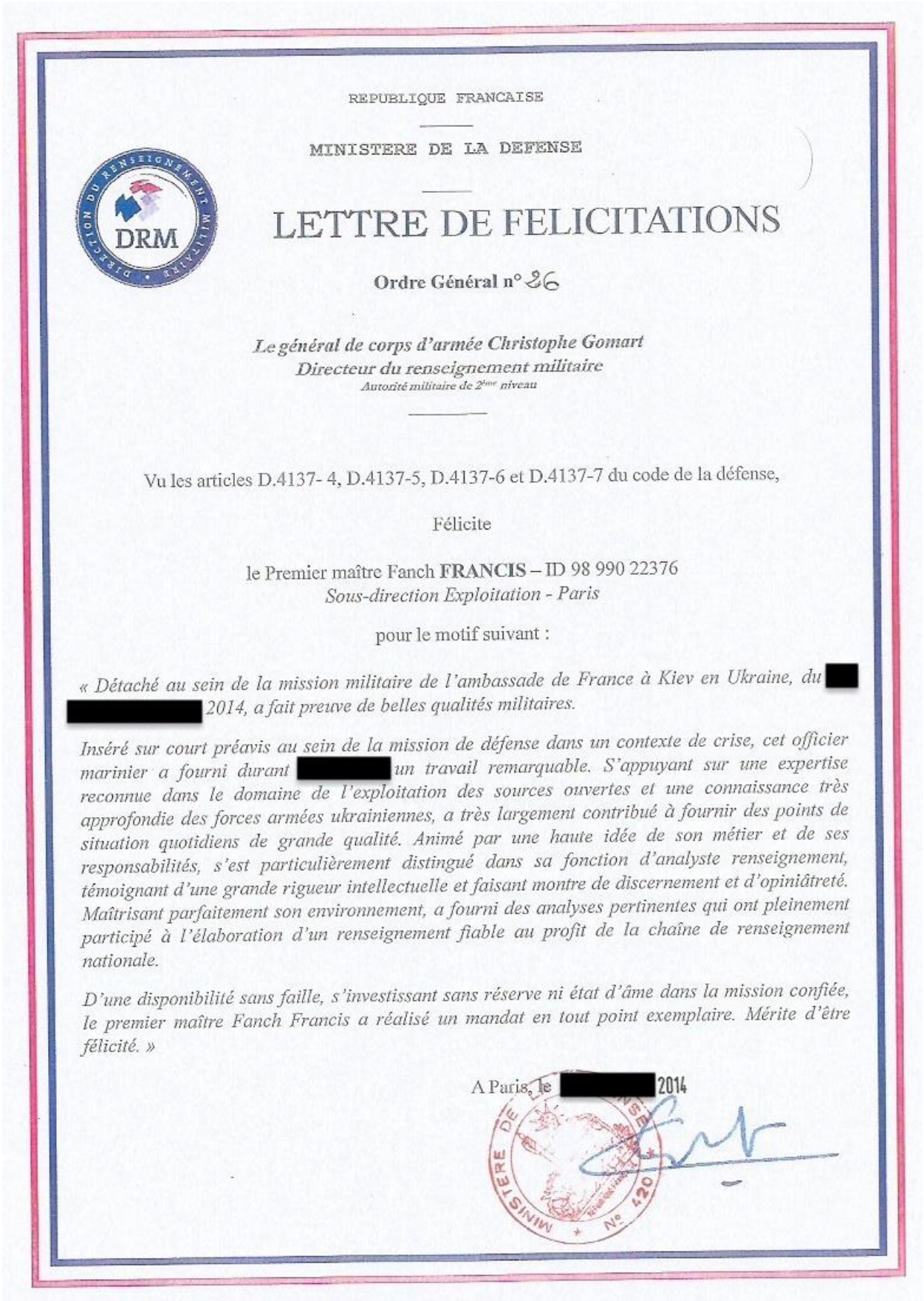
régulation, comme en témoignent les affrontements en cours, la question se pose de trouver la manière de maintenir la confiance dans ce réseau tout en limitant les opérations qui s'y déroulent.

Sans maîtrise de l'information, il n'y a pas de maîtrise des évènements. N'a lieu que ce qui laisse une trace, alors que l'internet devient la mémoire du monde, il est pressant de s'assurer que les évènements du monde soient bien enregistrés. Outre ces perspectives sociales et politiques, ces travaux de thèse pourraient améliorer les bases de données d'évènements existantes dont la méthodologie reste basée sur le PEA classique. Il existe, en effet, de nombreux projets ayant pour objectif de compiler les évènements dans des bases de données spécialisées. Il s'agit de comprendre le cours de l'histoire et d'estimer l'impact des évènements sur l'économie et la sécurité. on peut notamment citer : la base de données Kansas Event Data System (KEDS) (Gerner et Schrodt,1996), l'Integrated Conflict Early Warning System (ICEWS) (O'Brien, 2010), et le Global Database of Events, Language, and Tone (GDELT) (Leetaru and Schrodt, 2013). Le projet GDELT lancé en 2013: « *est la base de données ouverte la plus vaste, la plus complète et la plus haute résolution jamais créée sur la société humaine. Elle prend en compte 250 millions d'évènements géoréférencés ayant eu lieu dans le monde les 30 dernières années. Cette base de données permet d'exploiter les liens entre les personnes, les organisations, les lieux, les thèmes et les émotions liés à ces événements*. (GDELT projet, 2019). Elle utilise le système d'encodage Conflict and Mediation Event Observations (CAMEO) (Gerner et al, 2008), mais des systèmes plus modernes utilisant l'intelligence artificielle tels que le système d'encodage Machine-learning Protest Event Data System (MPEDS) (Hanna, op.cit.) pourraient également lui être appliqué. GDELT est maintenant soutenue par le système Google Big Query. Quand on sait qu'une donnée qui n'apparaît pas dans la page de résultat du moteur de recherche de Google n'a quasiment aucune chance d'être vue par un utilisateur, on peut se demander si à terme un événement qui n'apparaît pas dans la base GDELT a vraiment eu lieu. Ces bases de données particulières, les « events databases » servent de référence mais que valent-elles si elles sont incomplètes ?

Lors de nos travaux nous avons cherché en vain certains évènements des séparatistes en Ukraine dans la base GDELT. Le fait que cette base se sert essentiellement de journaux en ligne pour compiler les évènements est un biais significatif. Le fait que tous les liens proposés soient en anglais, ce qui laisse supposer que la base se limiterait à la version en anglais des sites étrangers, en est un autre. Sur un théâtre connecté, nous avons pu observer que les réseaux sociaux étaient plus exhaustifs. Notre méthodologie affiche un meilleur taux de précision, de pertinence et de

rappel. S'il est encore possible qu'un évènement ait lieu aujourd'hui sans qu'il en soit fait la moindre mention sur un réseau social, au vu de l'évolution de l'internet cela relèvera bientôt de l'exception. Dans leur comparaison entre l'information disponible sur GDELT et sur un média socila chinois, Zhang et Pan observent différence très significative (Zhang et Pan, 2019). Leur Collective Action from Social Media (CASM) relève 12 662 événements quand GDELT n'en prend en compte que 266. La différence est expliquée par un contrôle de l'État sur la presse plus fort que celui sur les médias sociaux. Cependant il faut être en mesure d'en filtrer le bruit et mieux en structurer le contenu. La détection d'événement au travers des médias sociaux pour étalonner des bases d'évènements serait un exemple de projet multidisciplinaire innovant. L'analyse des données pourrait servir à l'interprétation de la géopolitique des évènements, et mettre à disposition une ressource réutilisable et de référence.

Annexe 1 : Lettre de félicitations



REPUBLIQUE FRANCAISE

MINISTERE DE LA DEFENSE

DRM

LETTRE DE FELICITATIONS

Ordre Général n° 26

Le général de corps d'armée Christophe Gomart
Directeur du renseignement militaire
Autorité militaire de 2ème niveau

Vu les articles D.4137- 4, D.4137-5, D.4137-6 et D.4137-7 du code de la défense,

Félicite

le Premier maître Fanch **FRANCIS** – ID 98 990 22376
Sous-direction Exploitation - Paris

pour le motif suivant :

« Détaché au sein de la mission militaire de l'ambassade de France à Kiev en Ukraine, du [redacted] 2014, a fait preuve de belles qualités militaires.

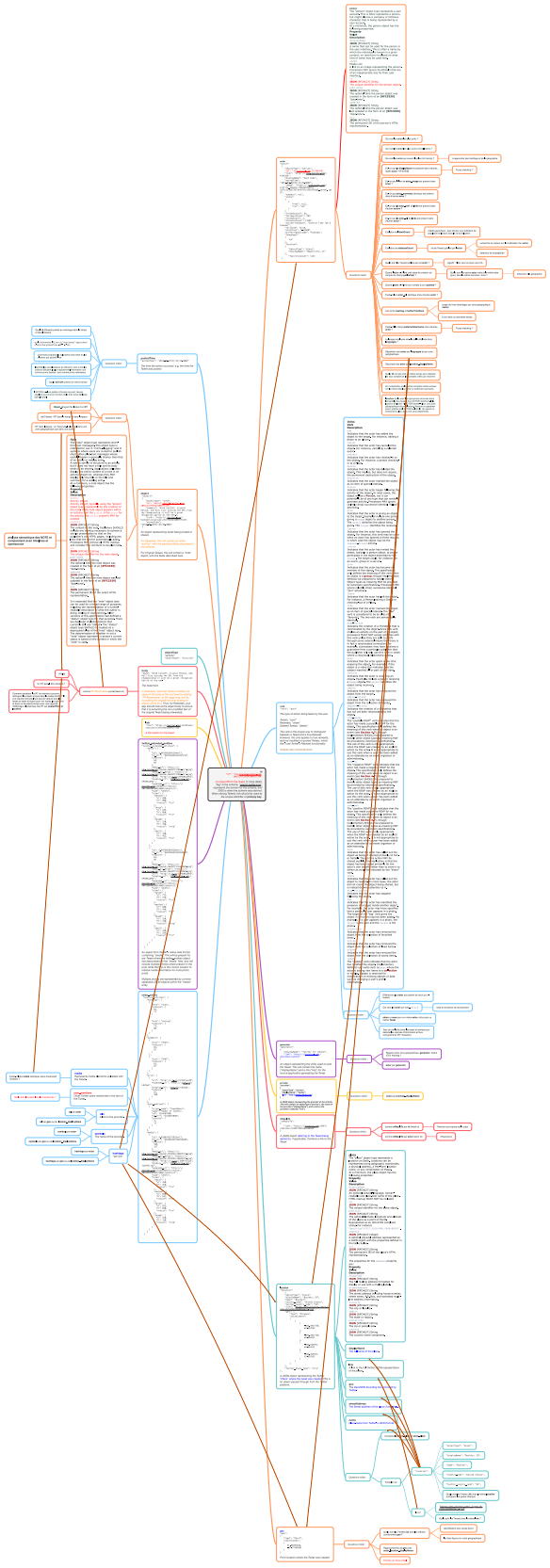
Inséré sur court préavis au sein de la mission de défense dans un contexte de crise, cet officier marinier a fourni durant [redacted] un travail remarquable. S'appuyant sur une expertise reconnue dans le domaine de l'exploitation des sources ouvertes et une connaissance très approfondie des forces armées ukrainiennes, a très largement contribué à fournir des points de situation quotidiens de grande qualité. Animé par une haute idée de son métier et de ses responsabilités, s'est particulièrement distingué dans sa fonction d'analyste renseignement, témoignant d'une grande rigueur intellectuelle et faisant montre de discernement et d'opiniâtreté. Maîtrisant parfaitement son environnement, a fourni des analyses pertinentes qui ont pleinement participé à l'élaboration d'un renseignement fiable au profit de la chaîne de renseignement nationale.

D'une disponibilité sans faille, s'investissant sans réserve ni état d'âme dans la mission confiée, le premier maître Fanch Francis a réalisé un mandat en tout point exemplaire. Mérite d'être félicité. »

A Paris, le [redacted] 2014

MINISTERE DE LA DEFENSE N° 420

Annexe 2 : Format TWITTER GNIP



Annexe 3 : Liste des toponymes filtres

Anglais	Ukrainien	Russe
Avdiivka	Авдіївка	Авдеевка
Almazna	Алмазна	Алмазная
Alchevsk	Алчевськ	Алчевск
Amvrosiivka	Амвросіївка	Амвросиевка
Antratsyt	Антрацит	
Apostolove	Апостолове	Апостолово
Artemivsk	Артемівськ	Артёмовск
Artemove	Артемове	Артёмово
Balakliia	Балаклія	Балаклея
Barvinkove	Барвінкове	Барвенково
Bakhmut	Бахмут	
Berdiansk	Бердянськ	
Beryslav	Берислав	
Bilytske	Білицьке	Белицкое
Bilozerske	Білозерське	Белозёрское
Bohodukhiv	Богодухів	Богодухов
Brianka	Брянка	Брянка
Valky	Валки	
Vasylivka	Василівка	Васильевка
Vakhrusheve	Вахрушеве	Вахрушево
Verkhivtseve	Верхівцеве	Верховцево
Verkhniodniprovsk	Верхньодніпровськ	Верхнеднепровск
Vilnohirsk	Вільногірськ	Вольногорск
Vilniansk	Вільнянськ	Вольнянск
Vovchansk	Вовчанськ	Волчанск
Volnovakha	Волноваха	**Волновахой**
Vuhlehirsk	Вуглегірськ	Углегорск
Vuhledar	Вугледар	Угледар
Henichesk	Генічеськ	Геническ
Hirnyk	Гірник	горняк
Hirske	Гірське	Горское
Hola Prystan	Гола Пристань	Голая Пристань
Horlivka	Горлівка	Горловка
Huliaipole	Гуляйполе	Гуляйполе
Debaltseve	Дебальцеве	Дебальцево
Derhachi	Дергачі	Дергачи
Dymytrov	Димитров	

Dniprodzerzhynsk	Дніпродзержинськ	Днепродзержинск
Dnipropetrovsk	Дніпропетровськ	Днепропетровск
Dniprorudne	Дніпрорудне	Днепрорудное
Dobropillia	Добропілля	Доброполье
Dokuchaievsk	Докучаєвськ	Докучаевск
Donetsk	Донецьк	Донецк
Druzhkivka	Дружківка	Дружковка
Enerhodar	Енергодар	
Yenakiieve	Єнакієве	Енакиево
Zhdanivka	Жданівка	Ждановка
Zhovti Vody	Жовті Води	Жёлтые Воды
Zaporizhia	Запоріжжя	Запорожье
Zelenodolsk	Зеленодольськ	Зеленодольск
Zymohiria	Зимогір'я	Зимогорье
Zmiiv	Зміїв	Змиёв
Zolote	Золоте	Золотое
Zorynsk	Зоринськ	Зоринск
Zuhres	Зугрес	Зугрэс
Izium	Ізюм	
Ilovaisk	Іловайськ	Иловайск
Kamianka-Dniprovska	Кам'янка-Дніпровська	Каменка-Днепровская
Kakhovka	Каховка	
Kiev	Київ	Kiev
Kirovsk	Кіровськ	Кировск
Kirovske	Кіровське	Кировское
Komsomolske	Комсомольське	Комсомольское
Kostiantynivka	Костянтинівка	Константиновка
Kramatorsk	Краматорськ	Краматорск
Krasnyi Luch	Красний Луч	Красный Луч
Krasnoarmiysk	Красноармійськ	Красноармейск
Krasnohorivka	Красногорівка	Красногоровка
Krasnohrad	Красноград	
Krasnodon	Краснодон	
Kreminna	Кремінна	Кременная
Kryvyi Rih	Кривий Ріг	Кривой Рог
Kupiansk	Куп'янськ	Купянск
Kurakhove	Курахове	Курахово
Lyman	Лиман	
Lysychansk	Лисичанськ	Лисичанск
Lozova	Лозова	Лозовая
Luhansk	Луганськ	Луганск
Lutuhyne	Лутугине	Лутугино
Liubotyn	Люботин	Люботин
Makiivka	Макіївка	Макеевка

Marhanets	Марганець	Марганец
Maryinka	Мар'їнка	Марьинка
Mariupol	Маріуполь	Мариуполь
Melitopol	Мелітополь	Мелитополь
Merefa	Мерефа	Мерефа
Mykolaivka	Миколаївка	Николаевка
Miusynsk	Міусинськ	Миусинск
Molodohvardiysk	Молодогвардійськ	Молодогвардейск
Molochansk	Молочанськ	Молочанск
Mospyne	Моспине	
Nikopol	Нікополь	Никополь
Nova Kakhovka	Нова Каховка	Новая Каховка
Novoazovsk	Новоазовськ	Новоазовск
Novohrodivka	Новогродівка	Новогродовка
Novodruzhesk	Новодружеськ	Новодружеск
Novomoskovsk	Новомосковськ	Новомосковск
Oleksandrivsk	Олександрівськ	Александровск
Orikhiv	Оріхів	Орехов
Pavlohrad	Павлоград	
Pervomaisk	Первомайськ	Первомайск
Pervomaiskyi	Первомайський	Первомайский
Perevalsk	Перевальск	Перевальск
Pereschepyne	Перещепине	Перещепино
Pershotravensk	Першотравенськ	Першотравенск
Petrovske	Петровське	Петровское
Pivdenne	Південне	Пивденное
Pidhorodne	Підгородне	Подгородное
Pokrov	Покров	
Polohy	Пологи	
Popasna	Попасна	Попасная
Pryvillia	Привілля	Приволье
Prymorsk	Приморськ	Приморск
Piatykhatky	П'ятихатки	Пятихатки
Rovenky	Ровеньки	Ровеньки
Rodynske	Родинське	Родинское
Rubizhne	Рубіжне	Рубежное
Svatove	Сватове	Сватово
Sverdlovsk	Свердловськ	**Свердловск**
Svitlodarsk	Світлодарськ	Светлодарск
Sviatohirsk	Святогірськ	Святогорск
Selydove	Селидове	Селидово
Sieverodonetsk	Сєвєродонецьк	Северодонецк
Synelnykove	Синельникове	Синельниково
Siversk	Сіверськ	Северск
Skadovsk	Скадовськ	Скадовск

Sloviansk	Слов'янськ	Славянск
Snizhne	Сніжне	Снежное
Soledar	Соледар	
Starobilsk	Старобільськ	Старобельск
Stakhanov	Стаханов	
Sukhodilsk	Суходільськ	Суходольск
Tavriysk	Таврійськ	Таврийск
Teplohirsk	Теплогірськ	Ирмино
Ternivka	Тернівка	Терновка
Tokmak	Токмак	
Torez	Торез	
Toretsk	Торецьк	Торецк
Ukrainsk	Українськ	Украинск
Kharkiv	Харків	Харьков
Khartsyzk	Харцизьк	Харцызск
Kherson	Херсон	
Tsiurupynsk	Цюрупинськ	Цюрупинск
Chasiv Yar	Часів Яр	Часов Яр
Chervonopartyzansk	Червонопартизанськ	Червонопартизанск
Chuhuiv	Чугуїв	Чугуев
Shakhtarsk	Шахтарськ	Шахтёрск
Schastia	Щастя	счастье
Yunokomunarivsk	Юнокомунарівськ	Юнокоммунаровск
Yasynuvata	Ясинувата	Ясиноватая

Annexe 4 : Codebook

1. Codebook : activités de l'opposition

Accuse	CLASSIFIER :	обвинять
Accused	CLASSIFIER :	обвиняемый
Activist	CLASSIFIER :	активист
Allege	CLASSIFIER :	утверждать
Alleged	CLASSIFIER :	Предполагаемая
Ammunition	CLASSIFIER :	амуниция
Amnesty	CLASSIFIER :	амнистия
Angered	CLASSIFIER :	Возмущенный
Armed	CLASSIFIER :	вооруженный
Arrest	CLASSIFIER :	арестовывать
Arrest	CLASSIFIER :	задержание
Arrested	CLASSIFIER :	арестованный
Arson	CLASSIFIER :	поджог
Assault	CLASSIFIER :	нападение
Assaulted	CLASSIFIER :	Нападение
Attack	CLASSIFIER :	Атака
Attacking	CLASSIFIER :	нападающий
Attempted	CLASSIFIER :	попытка
Attendee	CLASSIFIER :	Слушатель
Banner	CLASSIFIER :	Баннер
Banner	CLASSIFIER :	знамя
Beaten	CLASSIFIER :	избитый
Beating	CLASSIFIER :	битье
Blame	CLASSIFIER :	порицание
Blamed	CLASSIFIER :	обвиняют
Bloc	CLASSIFIER :	блок
Block	CLASSIFIER :	блок
Blockade	CLASSIFIER :	блокада
Blocked	CLASSIFIER :	блокированный
Blocking	CLASSIFIER :	блокировка
Blocking	CLASSIFIER :	блокирующий
Bloody	CLASSIFIER :	Кровавый
Boycott	CLASSIFIER :	Бойкотировать
Brutality	CLASSIFIER :	зверство
Bullet	CLASSIFIER :	пуля
Burn	CLASSIFIER :	жечь
Camp	CLASSIFIER :	Лагерь

Camp	CLASSIFIER :	команда
Campaigner	CLASSIFIER :	служака
Cancellation	CLASSIFIER :	отмена
Cannon	CLASSIFIER :	пушка
Censorship	CLASSIFIER :	цензура
Chant	CLASSIFIER :	песнопение
Chanting	CLASSIFIER :	Воспевание
Civilian	CLASSIFIER :	штатский
Clash	CLASSIFIER :	столкновение
Clinic	CLASSIFIER :	Клиника
Condemn	CLASSIFIER :	порицать
Condemned	CLASSIFIER :	осужденный
Converge	CLASSIFIER :	Converge
Corruption	CLASSIFIER :	коррупция
Counter	CLASSIFIER :	счетчик
Coup	CLASSIFIER :	переворот
Criticise	CLASSIFIER :	критиковать
Crowd	CLASSIFIER :	Толпа
Defect	CLASSIFIER :	дефект
Delegation	CLASSIFIER :	Делегация
Demand	CLASSIFIER :	требовать
Demand	CLASSIFIER :	спрос
Demanding	CLASSIFIER :	требовательный
Demolition	CLASSIFIER :	снос
Demonstration	CLASSIFIER :	демонстрация
Demonstrator	CLASSIFIER :	демонстратор
Denounce	CLASSIFIER :	Денонсировать
Detain	CLASSIFIER :	задержала
Detainee	CLASSIFIER :	задержанный
Detention	CLASSIFIER :	Заключение под стражу
Detention	CLASSIFIER :	арест
Dictator	CLASSIFIER :	диктатор
Discontent	CLASSIFIER :	Недовольство
Dismissal	CLASSIFIER :	отставка
Disobedience	CLASSIFIER :	непослушание
Dispersal	CLASSIFIER :	рассредоточение
Disperse	CLASSIFIER :	Рассеивать
Disrupt	CLASSIFIER :	срывать
Disrupted	CLASSIFIER :	Нарушается
Erupt	CLASSIFIER :	прорезываться
Escalate	CLASSIFIER :	обострять
Evict	CLASSIFIER :	выселять
Excessive	CLASSIFIER :	излишний
Eyewitness	CLASSIFIER :	очевидец
Fence	CLASSIFIER :	ограда

Fire	CLASSIFIER :	Пожар
Firing	CLASSIFIER :	обжиг
Flag	CLASSIFIER :	Флаг
Footage	CLASSIFIER :	метраж
Forcibly	CLASSIFIER :	принудительно
Gas	CLASSIFIER :	газ
Gathered	CLASSIFIER :	собранный
Gathering	CLASSIFIER :	сбор
Government	CLASSIFIER :	Правительство
Grievance	CLASSIFIER :	обида
Grievance	CLASSIFIER :	жалоба
Guardsman	CLASSIFIER :	гвардеец
Gunman	CLASSIFIER :	бандит
Gunshot	CLASSIFIER :	Огнестрельное
Harassed	CLASSIFIER :	беспокоили
Harassment	CLASSIFIER :	домогательство
Harassment	CLASSIFIER :	раздражение
Hose	CLASSIFIER :	Шланг
Hospitalize	CLASSIFIER :	госпитализировать
Imprisonment	CLASSIFIER :	Лишение свободы
Inauguration	CLASSIFIER :	инаугурация
Incident	CLASSIFIER :	инцидент
Incite	CLASSIFIER :	Подстрекают
Injure	CLASSIFIER :	ранить
Injured	CLASSIFIER :	Ранен
Injustice	CLASSIFIER :	несправедливость
Intimidate	CLASSIFIER :	Запугивание
Jail	CLASSIFIER :	тюремное заключение
Jailed	CLASSIFIER :	Заключенный
Junta	CLASSIFIER :	Хунта
Killing	CLASSIFIER :	Убийство
Killing	CLASSIFIER :	убой
Killing	CLASSIFIER :	Убийство
Looting	CLASSIFIER :	Грабежи
Loyalist	CLASSIFIER :	верноподданный
Makeshift	CLASSIFIER :	импровизированный
March	CLASSIFIER :	марш
Marching	CLASSIFIER :	походный
Massacre	CLASSIFIER :	бойня
Massacre	CLASSIFIER :	избиение
Medic	CLASSIFIER :	медик
Military	CLASSIFIER :	военный
Mob	CLASSIFIER :	чернь
Mobilize	CLASSIFIER :	Мобилизовать
Obstruct	CLASSIFIER :	Obstruct

Occupy	CLASSIFIER :	оккупировать
Occupying	CLASSIFIER :	занимающий
Opposition	CLASSIFIER :	оппозиция
Opposition	CLASSIFIER :	противодействие
Oust	CLASSIFIER :	вытеснять
Outrage	CLASSIFIER :	безобразие
Outrage	CLASSIFIER :	издевательство
Overnight	CLASSIFIER :	с ночевкой
Paramilitary	CLASSIFIER :	военизированный
Peaceful	CLASSIFIER :	мирное
Persecution	CLASSIFIER :	гонение
Petition	CLASSIFIER :	петиция
Petrol	CLASSIFIER :	Бензин
Plaza	CLASSIFIER :	площадь
Pro	CLASSIFIER :	профессионал
Projectile	CLASSIFIER :	метательный
Protest	CLASSIFIER :	Акция протеста
Protester	CLASSIFIER :	протестующий
Protesting	CLASSIFIER :	Протестуя
Raid	CLASSIFIER :	набег
Rally	CLASSIFIER :	ралли
Rally	CLASSIFIER :	собрание
Refusal	CLASSIFIER :	Отказ
Regime	CLASSIFIER :	Режим
Repression	CLASSIFIER :	репрессия
Repression	CLASSIFIER :	подавление
Rights	CLASSIFIER :	права
Riot	CLASSIFIER :	буйство
Rubber	CLASSIFIER :	Резинка
Security	CLASSIFIER :	Безопасность
Shooting	CLASSIFIER :	стрельба
Shouting	CLASSIFIER :	крики
Skirmish	CLASSIFIER :	перепалка
Slogan	CLASSIFIER :	Лозунг
Smashed	CLASSIFIER :	Разбил
Smashing	CLASSIFIER :	Smashing
Sniper	CLASSIFIER :	снайпер
Solidarity	CLASSIFIER :	солидарность
Spark	CLASSIFIER :	искра
Spokesman	CLASSIFIER :	представитель
Spray	CLASSIFIER :	Спрей
Stage	CLASSIFIER :	стадия
Storm	CLASSIFIER :	Буря
Street	CLASSIFIER :	улица
Strike	CLASSIFIER :	удар

Supporter	CLASSIFIER :	приверженец
Supporter	CLASSIFIER :	сторонник
Suppression	CLASSIFIER :	подавление
Tactic	CLASSIFIER :	тактика
Tent	CLASSIFIER :	палатка
Tents	CLASSIFIER :	Палатки
Terrorist	CLASSIFIER :	террористический
Topple	CLASSIFIER :	опрокидывать
Unarmed	CLASSIFIER :	безоружный
Unconstitutional	CLASSIFIER :	неконституционный
Unrest	CLASSIFIER :	беспорядки
Uprising	CLASSIFIER :	восстание
Violation	CLASSIFIER :	Нарушение
Violent	CLASSIFIER :	насильственный
Violently	CLASSIFIER :	неистово
Vow	CLASSIFIER :	Клятва

2. Codebook : indicateur de mouvement ou de position

Mot (FR)	Mot (RU/UA)
CLASSIFICATEUR: parti à	CLASSIFIER:вышли на
CLASSIFICATEUR: sera à	CLASSIFIER:буде в
CLASSIFICATEUR: Je vais	CLASSIFIER:вирушаю на
CLASSIFICATEUR: sera envoyé à	CLASSIFIER:відправлятимуться на
CLASSIFICATEUR: TOUS A	CLASSIFIER:ВСЕ НА
CLASSIFICATEUR: TOUS A	CLASSIFIER:Всі на
CLASSIFICATEUR: Lève-toi	CLASSIFIER:вставай
CLASSIFIER: sortir à	CLASSIFIER:выход на
CLASSIFICATEUR: allons	CLASSIFIER:выходим
CLASSIFICATEUR: Allons-y	CLASSIFIER:Давайте к
CLASSIFICATEUR: Allez	CLASSIFIER:Едем
CLASSIFICATEUR: va à	CLASSIFIER:едет в
CLASSIFICATEUR: aller à	CLASSIFIER:еду в
CLASSIFICATEUR: Je vais	CLASSIFIER:еду на
CLASSIFICATEUR: Allez	CLASSIFIER:Едьте
CLASSIFICATEUR: aller à	CLASSIFIER:ехать в
CLASSIFICATEUR: monter sur	CLASSIFIER:ехать на
CLASSIFICATEUR: demain à	CLASSIFIER:завтра на
CLASSIFICATEUR: a conduit dans	CLASSIFIER:заехали в

CLASSIFICATEUR: appel	CLASSIFIER:закликають
CLASSIFICATEUR: maintenant sur	CLASSIFIER:зараз на
CLASSIFICATEUR: aller à	CLASSIFIER:идти на
CLASSIFICATEUR: Montez sur	CLASSIFIER:їдьте на
CLASSIFICATEUR: Je peux emmener	CLASSIFIER:Могу отвозить
CLASSIFICATEUR: sur le territoire	CLASSIFIER:на території
CLASSIFICATEUR: sont situés	CLASSIFIER:находятся
CLASSIFICATEUR: Encore une fois sur	CLASSIFIER:опять на
CLASSIFICATEUR: transféré à	CLASSIFIER:переехала в
CLASSIFICATEUR: Approche	CLASSIFIER:підійде
CLASSIFICATEUR: Approche de	CLASSIFIER:подходить на
CLASSIFICATEUR: Allez	CLASSIFIER:Поехал
CLASSIFICATEUR: appel sur	CLASSIFIER:позвать на
CLASSIFICATEUR: Je vais aller à	CLASSIFIER:пойду на
CLASSIFICATEUR: Entrez	CLASSIFIER:поступить в
CLASSIFICATEUR: arrive à	CLASSIFIER:прибуває на
CLASSIFICATEUR: arriver à	CLASSIFIER:прибувають на
CLASSIFICATEUR: arriver	CLASSIFIER:прибывать
CLASSIFICATEUR: Allez	CLASSIFIER:приедут
CLASSIFIER: lors d'un rassemblement	CLASSIFIER:на митинг
CLASSIFICATEUR: en soutien	CLASSIFIER:в поддержку
CLASSIFICATEUR: pour une démonstration	CLASSIFIER:на демонстрацию
CLASSIFICATEUR: en marche	CLASSIFIER:на марш
CLASSIFICATEUR: processions en	CLASSIFIER:шествия в
CLASSIFICATEUR: appelle	CLASSIFIER:призывает на
CLASSIFICATEUR: Allez	CLASSIFIER:Приезжайте
CLASSIFICATEUR: venu à	CLASSIFIER:приїхав до
CLASSIFIER: est venu avec	CLASSIFIER:пришел с
CLASSIFICATEUR: Allez	CLASSIFIER:пришли
CLASSIFICATEUR: ils le font	CLASSIFIER:пробираются
CLASSIFICATEUR: protester contre	CLASSIFIER:протести на
CLASSIFICATEUR: Rouler	CLASSIFIER:рулим в
CLASSIFICATEUR: suivant	CLASSIFIER:рядом
CLASSIFICATEUR: emménage	CLASSIFIER:свозит в
CLASSIFICATEUR: Bientôt disponible	CLASSIFIER:Скоро в
CLASSIFICATEUR: Venir à	CLASSIFIER:собираться на
CLASSIFICATEUR: Allez	CLASSIFIER:спускаємося на

CLASSIFICATEUR: descendre	CLASSIFIER:спускаются
CLASSIFICATEUR: descendre	CLASSIFIER:спускаются
CLASSIFICATEUR: Immédiatement le	CLASSIFIER:сразу на
CLASSIFICATEUR: voir	CLASSIFIER:увидеть
CLASSIFICATEUR: Je suis allé à	CLASSIFIER:Ходил на
CLASSIFICATEUR: Je suis sur	CLASSIFIER:Я на

3. Codebook : indicateurs d'actes violents

Mot FR	Mot (UA)	Mot (RU)
CLASSIFICATEUR: révolution	CLASSIFIER:революція	CLASSIFIER:революция
CLASSIFICATEUR: groupe armé	CLASSIFIER:«ОЗБРОЄНА ГРУПА»	CLASSIFIER:ВООРУЖЕННАЯ ГРУППА
CLASSIFICATEUR: abattu	CLASSIFIER:застрелений	CLASSIFIER:застрелен
CLASSIFICATEUR: opposition	CLASSIFIER:ПРОТИСТОЯННЯ	CLASSIFIER:ПРОТИВОСТОЯНИЕ
CLASSIFICATEUR: AGRESSION	CLASSIFIER:АГРЕССИЯ	CLASSIFIER:АГРЕССИЯ
CLASSIFICATEUR: ALERTE	CLASSIFIER:ALERT	CLASSIFIER:ALERT
CLASSIFICATEUR: ARMES	CLASSIFIER:ЗБРОЯ	CLASSIFIER:ОРУЖИЕ
CLASSIFICATEUR: attaquants	CLASSIFIER:нападники	CLASSIFIER:нападавшие
CLASSIFICATEUR: attaque	CLASSIFIER:НАПАД	CLASSIFIER:НАПАДЕНИЕ
CLASSIFICATEUR: BLESSURES	CLASSIFIER:ТРАВМИ	CLASSIFIER:ТРАВМЫ
CLASSIFICATEUR: LUTTE	CLASSIFIER:БОРОТЬБА	CLASSIFIER:БОРЬБА
CLASSIFICATEUR: CONFLIT	CLASSIFIER:КОНФЛІКТ	CLASSIFIER:КОНФЛИКТ
CLASSIFICATEUR: est sélectionné	CLASSIFIER:У обране	CLASSIFIER:В избранное
CLASSIFICATEUR: COUVERTURE	CLASSIFIER:ПОКРИТТЯ	CLASSIFIER:ПОКРЫТИЕ
CLASSIFICATEUR: CRIMES	CLASSIFIER:ЗЛОЧИНИ	CLASSIFIER:ПРЕСТУПЛЕНИЯ
CLASSIFICATEUR: DANGEREUX	CLASSIFIER:НЕБЕЗПЕЧНО	CLASSIFIER:ОПАСНО
CLASSIFICATEUR: Fuite	CLASSIFIER:витоків	CLASSIFIER:УТЕЧЕК
CLASSIFICATEUR: MORT	CLASSIFIER:СМЕРТЬ	CLASSIFIER:СМЕРТЬ
CLASSIFIER: une explosion	CLASSIFIER:вибух	CLASSIFIER:взрыв
CLASSIFICATEUR: retarder	CLASSIFIER:прострочення	CLASSIFIER:просрочка
CLASSIFICATEUR: dénoncer	CLASSIFIER:денонсувати	CLASSIFIER:денонсировать
CLASSIFICATEUR: RETRAIT	CLASSIFIER:ВИДАЛЕННЯ	CLASSIFIER:УДАЛЕНИЕ
CLASSIFICATEUR: VICTIMES	CLASSIFIER:ВИБУХИ	CLASSIFIER:ВЗРЫВЫ
CLASSIFICATEUR: ÉVÉNEMENTS	CLASSIFIER:ПОДІЇ	CLASSIFIER:ПРОИСШЕСТВИЯ
CLASSIFICATEUR: INTERVIEW	CLASSIFIER:ВТРУЧАННЯ	CLASSIFIER:ВМЕШАТЕЛЬСТВО
CLASSIFICATEUR: KALASHNIKOV	CLASSIFIER:КАЛАШНИКОВ	CLASSIFIER:КАЛАШНИКОВ
CLASSIFICATEUR: à emporter	CLASSIFIER:відвезти	CLASSIFIER:увезти
CLASSIFICATEUR: nuisible	CLASSIFIER:шкідливе	CLASSIFIER:ВРЕДОНОСНАЯ
CLASSIFICATEUR: MENACE	CLASSIFIER:ЗАГРОЗА	CLASSIFIER:УГРОЗА

CLASSIFICATEUR: INTÉGRITÉ	CLASSIFIER:ВБИВСТВО	CLASSIFIER:УБИЙСТВО
CLASSIFICATEUR: MORT	CLASSIFIER:СМЕРТЬ	CLASSIFIER:СМЕРТЬ
CLASSIFICATEUR: munitions	CLASSIFIER:БОЄПРИПАСИ	CLASSIFIER:БОЕПРИПАСЫ
CLASSIFICATEUR: TRAVAIL	CLASSIFIER:РОБОТА	CLASSIFIER:РАБОТА
CLASSIFICATEUR: engagement	CLASSIFIER:заручник	CLASSIFIER:Заложник
CLASSIFICATEUR: AVERTISSEMENT	CLASSIFIER:ПОРУШЕННЯ	CLASSIFIER:НАРУШЕНИЯ
CLASSIFICATEUR: transmettre	CLASSIFIER:ПЕРЕСЛІДУВАННЯ	CLASSIFIER:ПРЕСЛЕДОВАНИЕ
CLASSIFICATEUR: REBELLION	CLASSIFIER:ПОВСТАННЯ	CLASSIFIER:ВОССТАНИЕ
CLASSIFICATEUR: FORCE	CLASSIFIER:НАПРУГУ	CLASSIFIER:НАПРЯЖЕНИЕ
CLASSIFICATEUR: TERRORISME	CLASSIFIER:ТЕРОРИЗМУ	CLASSIFIER:ТЕРРОРИЗМА
CLASSIFICATEUR: CAMP	CLASSIFIER:КАДРИ	CLASSIFIER:КАДРЫ
CLASSIFICATEUR: TUER	CLASSIFIER:ВБИТИ	CLASSIFIER:УБИТЬ
CLASSIFICATEUR: VICTIMES	CLASSIFIER:ЖЕРТВА	CLASSIFIER:ЖЕРТВА
CLASSIFICATEUR: VIOL	CLASSIFIER:ЗҐВАЛТУВАННЯ	CLASSIFIER:ИЗНАСИЛОВАНИЕ
CLASSIFICATEUR: VIOLENCE	CLASSIFIER:НАСИЛЬСТВО	CLASSIFIER:НАСИЛИЕ

4. Codebook : indicateur d'activités des forces ukrainiennes

CLASSIFICATEUR: Garde nationale	CLASSIFIER:национальная гвардия
CLASSIFICATEUR: SBU	CLASSIFIER:сбу
CLASSIFICATEUR: Aigle royal	CLASSIFIER:беркут
CLASSIFICATEUR: alpha	CLASSIFIER:альфа
CLASSIFICATEUR: Guépard	CLASSIFIER:Гепард
CLASSIFICATEUR: Tigre	CLASSIFIER:Тигр
CLASSIFICATEUR: Omega	CLASSIFIER:Омега
CLASSIFICATEUR: Scorpion	CLASSIFIER:Скорпион
CLASSIFICATEUR: Falcon	CLASSIFIER:Сокол
CLASSIFICATEUR: Cobra	CLASSIFIER:Кобра
CLASSIFICATEUR: Griffin	CLASSIFIER:Грифон
CLASSIFICATEUR: Jaguar	CLASSIFIER:Ягуар
CLASSIFICATEUR: Titan	CLASSIFIER:Титан
CLASSIFICATEUR: Léopard	CLASSIFIER:Барс
CLASSIFICATEUR: Skat	CLASSIFIER:Скат
CLASSIFICATEUR: Forces spéciales OMBRE	CLASSIFIER:Спецподразделение Тень
CLASSIFICATEUR: Forces spéciales LAVANDE	CLASSIFIER:спецподразделение Лаванда
CLASSIFICATEUR: Vega	CLASSIFIER:Вега
CLASSIFICATEUR: Phoenix	CLASSIFIER:Феникс
CLASSIFICATEUR: Kropyvnytskyi 3ème Régiment de forces spéciales autonome	CLASSIFIER:Кропивницкий 3-й отдельный полк спецназначения

CLASSIFICATEUR: 3ème régiment autonome des forces spéciales	CLASSIFIER:3-й отдельный полк спецназначения
CLASSIFICATEUR: 1ère division aéromobile	CLASSIFIER:1-я аэромобильная дивизия
CLASSIFICATEUR: 1ère division de la garde nationale de l'Ukraine	CLASSIFIER:1-я дивизия Национальной гвардии Украины
CLASSIFICATEUR: 6ème division de la garde nationale de l'Ukraine	CLASSIFIER:6-я дивизия Национальной гвардии Украины
CLASSIFICATEUR: 8ème brigade spéciale autonomee	CLASSIFIER:8-я отдельная бригада специального назначения
CLASSIFICATEUR: 9e brigade d'intervention spéciale autonomee	CLASSIFIER:9-я отдельная бригада специального назначения
CLASSIFICATEUR: 10ème brigade d'assaut de montagne	CLASSIFIER:10-я горно-штурмовая бригада
CLASSIFICATEUR: 10ème brigade spéciale	CLASSIFIER:10-я отдельная бригада специального назначения
CLASSIFICATEUR: 14e Brigade de radio-ingénierie de défense aérienne d'Ukraine	CLASSIFIER:14-я радиотехническая бригада ПВО Украины
CLASSIFICATEUR: 17ème régiment de la garde nationale de l'Ukraine	CLASSIFIER:17-й полк Национальной гвардии Украины
CLASSIFICATEUR: 24ème brigade mécanisée autonomee	CLASSIFIER:24-я отдельная механизированная бригада
CLASSIFICATEUR: 25ème brigade aéroportée distincte de Dnepropetrovsk	CLASSIFIER:25-я отдельная Днепропетровская воздушно-десантная бригада
CLASSIFICATEUR: 44ème brigade d'artillerie autonomee	CLASSIFIER:44-я отдельная артиллерийская бригада
CLASSIFICATEUR: 45ème brigade d'assaut aérien autonomee	CLASSIFIER:45-я отдельная десантно-штурмовая бригада
CLASSIFICATEUR: 46ème brigade d'assaut aérien autonomee	CLASSIFIER:46-я отдельная десантно-штурмовая бригада
CLASSIFICATEUR: 79ème Brigade d'Assaut autonomee	CLASSIFIER:79-я отдельная десантно-штурмовая бригада
CLASSIFICATEUR: 80ème brigade d'assaut aérien autonomee	CLASSIFIER:80-я отдельная десантно-штурмовая бригада
CLASSIFICATEUR: 81ème brigade aéromobile autonomee	CLASSIFIER:81-я отдельная аэромобильная бригада
CLASSIFICATEUR: 92ème brigade mécanisée autonomee	CLASSIFIER:92-я отдельная механизированная бригада
CLASSIFICATEUR: 95ème brigade d'assaut aérien autonomee	CLASSIFIER:95-я отдельная десантно-штурмовая бригада
CLASSIFICATEUR: 97ème division de carabine des gardes	CLASSIFIER:97-я гвардейская стрелковая дивизия
CLASSIFICATEUR: 801ème escouade anti-PDSS	CLASSIFIER:801-ый отряд по борьбе с ПДСС
CLASSIFICATEUR: 801e okremiy zagin borotby s PDSZ	CLASSIFIER:801-й окремий загін боротьби з ПДСЗ
CLASSIFICATEUR: Bataillon indépendant	CLASSIFIER:независимый батальон

CLASSIFICATEUR: bataillon de l'Azov	CLASSIFIER:батальон Азов
CLASSIFICATEUR: bataillon	CLASSIFIER:батальон
CLASSIFICATEUR: SMAP	CLASSIFIER:ПСМОП
CLASSIFICATEUR: Tempête	CLASSIFIER:Шторм
CLASSIFICATEUR: Sich	CLASSIFIER:Січ
CLASSIFICATEUR: Police spéciale	CLASSIFIER:Специальная полиция
CLASSIFICATEUR: Ministères de l'intérieur	CLASSIFIER:министерства внутренних дел
CLASSIFICATEUR: Bataillon "Kiev-1"	CLASSIFIER:Батальон «Киев-1»
CLASSIFICATEUR: Bataillon "Kiev-2"	CLASSIFIER:Батальон «Киев-2»
CLASSIFICATEUR: Bataillon Dnepr-1	CLASSIFIER:Батальон «Днепр-1»
CLASSIFICATEUR: Bataillon de maintien de la paix	CLASSIFIER:Батальон «Миротворец»
CLASSIFICATEUR: Artyomovsk	CLASSIFIER:«Артемовск»
CLASSIFICATEUR: APU	CLASSIFIER: ВСУ
CLASSIFICATEUR: 25ème brigade tactique	CLASSIFIER:25-та повітрянодесантна бригада
CLASSIFICATEUR: SBU	CLASSIFIER:СБУ
CLASSIFICATEUR: Groupe "A"	CLASSIFIER:Группа «А»
CLASSIFICATEUR: AIM d'Ukraine	CLASSIFIER:МВС України
CLASSIFICATEUR: MIA	CLASSIFIER:МВД
CLASSIFICATEUR: Garde nationale	CLASSIFIER:Национальная гвардия
CLASSIFICATEUR: VV MIF d'Ukraine	CLASSIFIER:ВВ МВС України
CLASSIFICATEUR: Spetspidrozdil	CLASSIFIER:Спецпідрозділ
CLASSIFICATEUR: DOS	CLASSIFIER:ОСН
CLASSIFICATEUR: sauvegarde	CLASSIFIER:резервный
CLASSIFICATEUR: police de la circulation	CLASSIFIER:ГАИ
CLASSIFICATEUR: APU	CLASSIFIER:ВСУ
CLASSIFICATEUR: ATS	CLASSIFIER:ОВДБ
CLASSIFICATEUR: bataillon de Dzhokhar Dudayova	CLASSIFIER:батальон Джохара Дудаєва
CLASSIFICATEUR: OUN	CLASSIFIER:ОУН
CLASSIFICATEUR: DUK Right Sector	CLASSIFIER:ДУК Правый сектор
CLASSIFICATEUR: DBTO Donbass	CLASSIFIER:ДБТО Донбасс
CLASSIFICATEUR: Karpatska Sich	CLASSIFIER:Карпатська Січ
CLASSIFICATEUR: Squad Chase	CLASSIFIER:Отряд Погоня
CLASSIFICATEUR: OGD Libre Caucase	CLASSIFIER:ОПД Свободный Кавказ
CLASSIFICATEUR: GNL	CLASSIFIER:ГНЛ
CLASSIFICATEUR: 25ème brigade aéroportée distincte de Dnepropetrovsk	CLASSIFIER:25-я отдельная Днепропетровская воздушно-десантная бригада
CLASSIFICATEUR: 79ème brigade aéromobile autonomee	CLASSIFIER:79-я отдельная аэромобильная бригада
CLASSIFICATEUR: 80-a brigade aérienne	CLASSIFIER:80-а аеромобільна бригада
CLASSIFICATEUR: 80ème brigade d'assaut aérien autonomee	CLASSIFIER:80-я отдельная десантно-штурмовая бригада

CLASSIFICATEUR: brigade de la foule de 95 avions	CLASSIFIER:95-а аеромобільна бригада
CLASSIFICATEUR: 95ème brigade d'assaut aérien autonomee	CLASSIFIER:95-я отдельная десантно-штурмовая бригада
CLASSIFICATEUR: 11ème brigade d'aviation de l'armée autonomee	CLASSIFIER:11-я отдельная бригада армейской авиации
CLASSIFICATEUR: 16ème brigade d'aviation de l'armée autonomee	CLASSIFIER:16-я отдельная бригада армейской авиации
CLASSIFICATEUR: 24ème fer pour eux. Prince Danila Galitsky brigade mécanisée autonomee	CLASSIFIER:24-я железная им. князя Данилы Галицкого отдельная механизированная бригада
CLASSIFICATEUR: 28ème brigade mécanisée de gardes autonomes	CLASSIFIER:28-я отдельная гвардейская механизированная бригада
CLASSIFICATEUR: 30ème garde autonomee	CLASSIFIER:30-я отдельная гвардейская
CLASSIFICATEUR: 51ème brigade mécanisée autonomee	CLASSIFIER:51-я отдельная механизированная бригада
CLASSIFICATEUR: 72ème brigade mécanisée autonomee	CLASSIFIER:72-я отдельная механизированная бригада
CLASSIFICATEUR: 92ème autonome Mécanisé	CLASSIFIER:92-я отдельная механизированная
CLASSIFICATEUR: 93ème autonome Mécanisé	CLASSIFIER:93-я отдельная механизированная
CLASSIFICATEUR: 101ème brigade de sécurité distincte de l'état-major des forces armées ukrainiennes	CLASSIFIER:101-я отдельная бригада охраны Генерального штаба Вооружённых сил Украины
CLASSIFICATEUR: 128ème brigade minière autonomee	CLASSIFIER:128-я отдельная горнопехотная бригада
CLASSIFICATEUR: 1ère brigade de chars autonomee	CLASSIFIER:1-я отдельная танковая бригада
CLASSIFICATEUR: 27ème Régiment d'artillerie de roquettes	CLASSIFIER:27-й реактивный артиллерийский полк
CLASSIFICATEUR: 17ème brigade de chars	CLASSIFIER:17-а танкова бригада
CLASSIFICATEUR: 17ème brigade de chars autonomee	CLASSIFIER:17-я отдельная танковая бригада
CLASSIFICATEUR: 26ème brigade d'artillerie	CLASSIFIER:26-я артиллерийская бригада
CLASSIFICATEUR: 44ème brigade d'artillerie autonomee	CLASSIFIER:44-я отдельная артиллерийская бригада
CLASSIFICATEUR: 55ème brigade d'artillerie autonomee	CLASSIFIER:55-я отдельная артиллерийская бригада
CLASSIFICATEUR: 15ème brigade d'aviation de transport autonomee	CLASSIFIER:15-я отдельная бригада транспортной авиации
CLASSIFICATEUR: 3ème régiment autonome à vocation spéciale	CLASSIFIER:3-й отдельный полк специального назначения
CLASSIFICATEUR: 8ème régiment autonome à vocation spéciale	CLASSIFIER:8-й отдельный полк специального назначения

CLASSIFICATEUR: 140ème centre des forces d'opérations spéciales	CLASSIFIER:140-й центр сил специальных операций
CLASSIFICATEUR: 54ème bataillon de reconnaissance autonome	CLASSIFIER:54-й отдельный разведывательный батальон
CLASSIFICATEUR: Unité militaire	CLASSIFIER:Воинская часть
CLASSIFICATEUR: Garde frontière	CLASSIFIER:Отдел пограничной службы
CLASSIFICATEUR: APC	CLASSIFIER:БТрО
CLASSIFICATEUR: Aydar	CLASSIFIER:Айдар
CLASSIFICATEUR: La 138ème brigade de radio-ingénierie de défense aérienne d'Ukraine	CLASSIFIER:138-я радиотехническая бригада ПВО Украины
CLASSIFICATEUR: 164ème brigade de radio-ingénierie de défense aérienne d'Ukraine	CLASSIFIER:164-я радиотехническая бригада ПВО Украины
CLASSIFICATEUR: Quartier général des forces armées ukrainiennes	CLASSIFIER:Генеральный штаб Вооружённых сил Украины
CLASSIFICATEUR: Corps ukrainien volontaire	CLASSIFIER:Добровольческий украинский корпус
CLASSIFICATEUR: Bataillon Donbas-Ukraine	CLASSIFIER:батальон Донбасс-Украина
CLASSIFICATEUR: bataillon OUN	CLASSIFIER:батальон ОУН
CLASSIFICATEUR: Sich Riflemen	CLASSIFIER:Сечевые стрельцы

5. Verbes liés à l’affrontement

Term	trad brute
утаить	dissimuler
замутиться	s'impliquer
поставиться	mettre en place
присоединять	attacher
охать	gémir
высылать	expulser
остановить	arrêter
толочь	marteler
занимать	occuper
заселить	occuper
допасти	pour finir
жариться	rôtir
ошарашить	choquer
прекратить	arrêter
закопать	enterrer

натянуть	tirer
ввалиться	tomber dans
пороть	claquer
шлепать	fesser
повредить	faire mal
разоружиться	désarmer
пресечь	arracher
колыхаться	vaciller
воспламениться	enflammer
гонять	conduire
нанести	appliquer
провести	tenir
простукивать	frapper
сметать	balayer
довороваться	être fini
репрессировать	réprimer
кристаллизовать	cristalliser
вовлечь	engager
выловить	attraper
замирать	mourir
замирять	pacifier
бомбиться	être bombardé
выпускать	libération
придавить	épingler
обессилеть	devenir faible
перевозить	porter
запрятать	se cacher
отключить	désactiver
притушить	éteindre
сфокусировать	se concentrer
фокусироваться	se concentrer
фальсифицировать	falsifier
рыдать	sanglot
заслать	envoyer
преодолевать	surmonter
учинить	infliger
подначивать	mettre en place
разрабатывать	développer
отклонять	rejeter
испепелить	incinérer
спуститься	descendre
язвить	faire claquer
причинять	provoquer
расстреливать	tirer
воспаляться	enflammer

передраться	se battre
целить	cibler
обтягивать	couvrir
содержаться	contenir
крыть	couvrir
завилять	vol stationnaire
вступить	rejoindre
зарывать	enterrer
выдвигать	pousser en avant
прокачать	saigner
восставать	rebelle
сшибить	abattre
скрыться	se cacher
агонизировать	agoniser
ослабевать	affaiblir
нарушать	casser
разрушать	détruire
разглагольствовать	se déchaîner
промедлить	retarder
упаковывать	meute
саботировать	sabotage
задействовать	engager
мешать	interférer
изнасиловать	violer
диверсифицировать	diversifier
вмешаться	intervenir
взбудоражить	exciter
рассердиться	se fâcher
прошлепать	fessée
утирать	essuyer
заготавливаться	stocké
бомбить	bombarder
растворяться	dissoudre
наказать	punir
придушить	étrangler
прокалывать	percer
скорбить	faire son deuil
заказывать	commander
откатывать	reculer
поддаваться	succomber
затерроризировать	terroriser
повоевать	faire la guerre
помститься	se venger
застрелить	tirer
пробомбить	bombarder

бушевать	faire rage
отползти	ramper
разоружать	désarmer
потолкаться	frapper
сторговаться	négocier
внедриться	s'infiltrer
обстрелять	tirer sur
освободить	libération
штурмовать	prendre d'assaut
напрягаться	pour forcer
пронизывать	pénétrer
обстреливать	tirer sur
выстрелить	tirer
сгрести	ratisser
утечь	fuir
разрушить	détruire
торпедировать	torpille
выкорчевывать	éradiquer
завоёвывать	conquérir
забиться	battre
ограничиваться	confiner
отбиваться	se battre
застучать	frapper
уползать	ramper
подмять	écraser
противодействовать	contrecarrer
лопнуть	éclater
вышагивать	le rythme
бомбардировать	bombarder
отстаивать	défendre
предавать	trahir
притянуться	tirer
переливаться	débordement
убежать	fuir
мобилизоваться	mobiliser
разворовать	piller
дробить	écraser
зарасти	envahir
подпереть	soutenir
подбить	assommer
поразить	frapper
вышибать	assommer
искоренить	éradiquer
проболеть	faire mal
сколотить	abattre

запечатлевать	pour capturer
взвести	armer
ошеломить	assommer
заколотить	pilonner
взорваться	exploser
мобилизовать	mobiliser
уморить	tuer
срыть	démolir
крушить	détruire
прирезать	massacre
рубать	abattre
уничтожать	détruire
урезаться	abattre
защищать	protéger
вышибить	assommer
поостыть	se calmer
пробивать	coup de poing
перестукиваться	abattre
доламывать	casser
ябедничать	débusquer
вдарить	battre dans
постреливать	tirer
защищаться	défendre
скостить	abattre
обезопасить	sécurisé
поддать	succomber
наломать	briser l'homme
распасться	se désintégrer
рубить	abattre
стрельнуть	tirer
задраить	se battre
снести	abattre
повелевать	commander
порубать	abattre
поддаться	succomber
взламывать	pirater
потоптаться	piétiner
маневрировать	manœuvrer
одолеть	battre
уничтожаться	être détruit
карать	punir
выслеживать	traquer
спикировать	abattre
поражать	frapper
угробить	ruiner

завертеть	bousiller
устаивать	périr
продержаться	tiens bon
аннигилировать	annihiler
избивать	tabasser
подуть	coup
отмереть	mourir
мобилизовывать	mobiliser
сникнуть	se battre
разбомбить	bombarder
заколотиться	pilonner
дестабилизировать	déstabiliser
похищаться	être kidnappé
затрубить	saigner
скоротать	décéder
расстрелять	tirer
преставиться	décéder
припасти	épargner
расквитаться	se venger
устоять	résister
покарать	punir
обезглавливать	décapiter
рушить	abattre
стрематься	lutter pour
исполняться	être exécuté
обводить	encerclant
пытать	torture
поквитаться	se venger
зверствовать	commettre des atrocités
выгнать	chasser
сбежать	fuir
избить	tabasser
кровоточить	saigner
дубасить	matraquer
застрелиться	se tirer une balle
согнать	chasser
терроризировать	terroriser
истреблять	exterminer
нейтрализовать	neutraliser
зарезать	massacre
застреливать	tirer
отстукивать	abattre
вредить	faire du mal
доломать	casser

зарубить	pirater
втаскивать	tirer dans
умертвить	tuer
помучить	torturer
заклать	massacre
искалечить	estropier
бороть	se battre
удариться	frapper
прострелить	tirer à travers
побить	battre
раздавливать	écraser
приостанавливаться	arrêter
вырубить	assommer
распинать	crucifier
сдетонировать	faire exploser
подглядывать	espion
покружить	encercler
облажаться	bousiller
сшибать	abattre
вдолбить	enfoncer
убегать	fuir
изрубить	abattre
попарить	abattre

Bibliographie

Abdallah-Sinno, May, Fadi Ahhmar, Nashwan M. Al-Sumairi, Caroline Angé, Florencio Ceballos, Chirine Ben Abdallah, Maryam Ben Salem, et al. 2013. *Les réseaux sociaux sur Internet à l'heure des transitions démocratiques*. Édité par Sihem Najar. Tunis, France, Tunisie: IRMC.

Abiteboul, Par Serge. 2018. « Les déclinaisons de la neutralité ». *Annales des Mines*, 5.

Aday, Sean, Henry Farrell, Marc Lynch, John Sides, et Deen Freelon. 2012. « Blogs and Bullets II: New Media and Conflict after the Arab Spring ». https://www.usip.org/publications/2012/07/blogs-and-bullets-ii-new-media-and-conflict-after-arab-spring.

Aday, Sean, Henry Farrell, Marc Lynch, John Sides, John Kelly, et Ethan Zuckerman. 2010. « Blogs and bullets: New media in contentious politics ». *United States Institute of Peace*, 1–31.

Adrian, Benjamin, Jörn Hees, Ivan Herman, Michael Sintek, et Andreas Dengel. 2010. « Epiphany: Adaptable RDFa Generation Linking the Web of Documents to the Web of Data ». In *Knowledge Engineering and Management by the Masses*, édité par Philipp Cimiano et H. Sofia Pinto, 178-92. Lecture Notes in Computer Science 6317. Springer Berlin Heidelberg. http://link.springer.com/chapter/10.1007/978-3-642-16438-5_13.

Alexander, Peter, Carin Runciman, et Boitumelo Maruping. 2016. « The use and abuse of police data in protest analysis South Africa's Incident Registration Information System (IRIS) ». *South African Crime Quarterly* 58 (1): 9-21-21. https://doi.org/10.17159/2413-3108/2016/v0n58a1513.

Allan, James. 2002. « Introduction to Topic Detection and Tracking ». In *Topic Detection and Tracking: Event-Based Information Organization*, édité par James Allan, 1-16. The Information Retrieval Series. Boston, MA: Springer US. https://doi.org/10.1007/978-1-4615-0933-2_1.

Alloing, Camille, Flavien Chantrel, Anne-Laure Raffestin, et Terry Zimmer. 2011. « Regards croisés sur la veille ». Text. juillet 2011. http://www.enssib.fr/bibliotheque-numerique/notices/49487-regards-croises-sur-la-veille.

Almeida, Paul. 2019. *Social Movements: The Structure of Collective Mobilization*. 1re éd. University of California Press. https://www.jstor.org/stable/j.ctvd1c7d7.

American Library Association. 2017a. « Digital Literacy ». *Welcome to ALA's Literacy Clearinghouse* (blog). 19 janvier 2017. https://literacy.ala.org/digital-literacy/.

———. 2017b. « Information Literacy ». *Welcome to ALA's Literacy Clearinghouse* (blog). 2 juillet 2017. https://literacy.ala.org/information-literacy/.

———. 2019. « About ALA ». Text. About ALA. 2019. http://www.ala.org/aboutala/.

« Analyse juridique de la loi « contre la haine en ligne » ». 2019. *La Quadrature du Net* (blog). 17 juin 2019. https://www.laquadrature.net/2019/06/17/analyse-juridique-de-la-loi-contre-la-haine-en-ligne/.

Andrejevic, Mark. 2017. « To Preempt a Thief », 18.

Andretta, Massimiliano, et Elena Pavan. 2018. « Mapping Protest on the Refugee Crisis: Insights from Online Protest Event Analysis ». In *Solidarity Mobilizations in the 'Refugee Crisis': Contentious Moves*, édité par Donatella della Porta, 299-324. Palgrave Studies in European Political Sociology. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-71752-4_11.

Araud, Gérard. 2019. « (20) Gérard Araud sur Twitter : “RT n’est pas une chaîne d’information. C’est l’instrument d’une puissance étrangère. Y apparaître, c’est en être complice. https://t.co/mr564KVuLK” / Twitter ». Twitter. 29 mars 2019. https://twitter.com/GerardAraud/status/1111753988913942528.

Asher, Jeff, et Rob Arthur. 2017. « Inside the Algorithm That Tries to Predict Gun Violence in Chicago ». *The New York Times*, 13 juin 2017, sect. The Upshot. https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html.

Aspen Institute. 2019. « The Aspen Institute - - Executive Summary ». 2019. http://csreports.aspeninstitute.org/Knight-Commission-TMD/2019/report/details/0283/Knight-Commission.

Assemblée Nationale. 16/10/ 18 c. « Audition du général Richard Lizurey, directeur général de la gendarmerie nationale, sur le projet de loi de finances pour 2019. » 16/10/ 18 c. http://www.assemblee-nationale.fr/15/cr-cdef/18-19/c1819009.asp.

———. 2013a. *LOI n° 2013-595 du 8 juillet 2013 d’orientation et de programmation pour la refondation de l’école de la République*. *2013-595*.

———. 2013b. *LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*. *2013-1168*.

———. 2018a. *Loi no 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense*. https://www.google.com/search?q=%22ambition+2030%22&oq=%22ambition+2030%22&aqs=chrome..69i57j0l5.6409j0j7&sourceid=chrome&ie=UTF-8.

———. 2018b. « Commission de la défense nationale et des forces armées ». session ordinaire de 2018-2019.

———. 2018c. « Assemblée nationale ~ Compte rendu de réunion de la commission de la défense nationale et des forces armées ». Compte rendu n° 9. http://www.assemblee-nationale.fr/15/cr-cdef/18-19/c1819009.asp.

———. 2019. *Texte adopté n° 310 - Proposition de loi visant à lutter contre les contenus haineux sur internet*. http://www.assemblee-nationale.fr/15/ta/ta0310.asp.

Assemblée Nationale, Assemblée. 2018d. « Défense : enjeux de la numérisation des armées ». 996. Asemblée nationale. http://www.assemblee-nationale.fr/dyn/15/dossiers/enjeux_numerisation_armees_rap-info.

Atefeh, Farzindar, et Wael Khreich. 2015. « A Survey of Techniques for Event Detection in Twitter: TECHNIQUES FOR EVENT DETECTION IN TWITTER ». *Computational Intelligence* 31 (1): 132-64. https://doi.org/10.1111/coin.12017.

Au Yeung, Ching Man, Nicholas Gibbins, et Nigel Shadbolt. 2008. « Collective User Behaviour and Tag Contextualisation in Folksonomies ». In , 659-62. http://eprints.soton.ac.uk/266990/.

Auckenthaler, Brice, Pierre d’Huy, et Philippe Lemoine. 2007. *L’imagination collective: créer et piloter des réseaux créatifs efficaces*. Rueil-Malmaison, France: Éd. Liaisons.

Babaei, Mahmoudreza, Przemyslaw Grabowicz, Isabel Valera, et Manuel Gomez-Rodriguez. 2015. « On the Users’ Efficiency in the Twitter Information Network ». In *Ninth International AAAI Conference on Web and Social Media*. http://www.aaai.org/ocs/index.php/ICWSM/ICWSM15/paper/view/10542.

Bachimont. 2006. « Qu’est-ce qu’une ontologie ? » 7 mars 2006. http://www.technolangue.net/imprimer.php3?id_article=280#targetText=Pour%20cela%2C%20il%20y%20a,ontologies%20dans%20une%20exploitation%20informatique.

Bachner, Jennifer. 2014. « Predictive Policing: Preventing Crime with Data and Analytics », 5.

Bagguley, Paul. 2010. « The Limits of Protest Event Data and Repertoires for the Analysis of Contemporary Feminism ». *Politics & Gender* 6 (4): 616-22. https://doi.org/10.1017/S1743923X10000401.
Bancaud, Delphine. 2016. « Un partenariat très polémique entre Microsoft et l'Education nationale ». *20 minutes*, septembre. https://www.20minutes.fr/societe/1925119-20160915-pourquoi-partenariat-entre-microsoft-education-nationale-fait-polemique.
Bargel, Lucie, et Anne-Sophie Petitfils. 2011. « Chapitre 10. Appropriations d'internet et trajectoires militantes «dans» et «en dehors» de l'UMP ». *Académique*, 187–199.
Barlette, Yves. 2013. *Impact des réseaux numériques dans les organisations*. Presses des MINES.
Barnes, Stuart, et Martin Böhringer. 2009. « Continuance usage intention in microblogging services: The case of Twitter ». http://aisel.aisnet.org/ecis2009/298/.
Bautès, Nicolas. 2012. « Rapports à l'espace, discours et portée politique de l'activisme urbain à Mumbai: l'initiative Urbz face à l'élargissement de l'arène publique ». *L'Information géographique* 76 (1): 89–89.
Bawden, David. 2001. « Information and Digital Literacies: A Review of Concepts ». *Journal of Documentation*, avril. https://doi.org/10.1108/EUM0000000007083.
Baygert, Nicolas. 2014. « L'activisme numérique au regard du consumérisme politique: Pirates et Tea Partiers sous la loupe ». *Participations*, no 1: 75–95.
BBC. 2014. « Ukraine Crisis: Timeline ». *BBC News*, 13 novembre 2014, sect. Europe. https://www.bbc.com/news/world-middle-east-26248275.
Beau, Francis. 2019. « Le renseignement au prisme des sciences de l'information ». Thesis, Valenciennes. http://www.theses.fr/2019VALE0006.
Becht, Olivier, et Thomas Gassiloud. 2018. « N° 996 - Rapport d'information de MM. Olivier Becht et Thomas Gassilloud déposé en application de l'article 145 du règlement, par la commission de la défense nationale et des forces armées, en conclusion des travaux d'une mission d'information sur les enjeux de la numérisation des armées ». 2018. http://www.assemblee-nationale.fr/15/rap-info/i0996.asp.
Beissinger, Mark R. 2011. « Mechanisms of Maidan: The Structure of Contingency in the Making of the Orange Revolution ». In .
Benford, Robert D., et David A. Snow. 2000. « Framing Processes and Social Movements: An Overview and Assessment ». *Annual Review of Sociology* 26 (1): 611-39. https://doi.org/10.1146/annurev.soc.26.1.611.
Benghozi, Pierre-Jean, et Michelle Bergadaà. 2012. *Les savoirs du web*. Bruxelles, Belgique: De Boeck, DL 2012.
Benkirane, Reda. 2012. « The Alchemy of Revolution: The Role of Social Networks and New Media in the Arab Spring ». GCSP Policy Paper 2012/7. Policy Paper. GCSP. http://www.archipress.org/docs/pdf/Alchemy_of_Revolution_RBenkirane.pdf.
Benvegnu, Nicolas. 2002. « La technique en usage l'introduction d'internet dans le répertoire de mobilisation électorale de candidats en campagne pour les élections législatives de juin 2002 ».
Bijker, Wiebe E. 2006. *Why and How Technology Matters*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199270439.003.0037.
Boileau. 1674. *ART POETIQUE. Epîtres, Odes, Poésies diverses et épigrammes*. Paris: Flammarion.
Boisset, Emmanuel. 2016. « Aperçu historique sur le mot événement ». In *Que m'arrive-t-il ? : Littérature et événement*, édité par Philippe Corno, 17-30. Interférences. Rennes: Presses universitaires de Rennes. http://books.openedition.org/pur/29783.
Boussad, Sonia. 2001. *L'usage d'internet par ATTAC Rouen: incidences sur le mode de militantisme traditionnel*. Paris, France: l'auteur.

Boyd, Danah. 2015. « Bibliography of Research on Social Network Sites ». 2015. http://www.danah.org/researchBibs/sns.php.
Bradshaw, Tim, et James Blitz. 2011. « NATO draws on Twitter for Libya strikes ». *Washington Post*, juin 2011.
Bratton, William J. 2011. « Reducing Crime through Prevention Not Incarceration: Imprisonment and Crime ». *Criminology & Public Policy* 10 (1): 63-68. https://doi.org/10.1111/j.1745-9133.2010.00688.x.
Breindl, Yana, et François FB Briatte. 2009. « Activisme sur internet et discours stratégiques autour de la propriété intellectuelle ». *Terminal* 103: 23–32.
Breslin, John G., Alexandre Passant, et Denny Vrandečić. 2011. « Social Semantic Web ». In *Handbook of Semantic Web Technologies*, édité par John Domingue, Dieter Fensel, et James A. Hendler, 467-506. Berlin, Heidelberg: Springer Berlin Heidelberg. http://link.springer.com/10.1007/978-3-540-92913-0_12.
Breuer, Anita. 2011. « Obstacles to citizen participation by direct democracy in Latin America: a comparative regional analysis of legal frameworks and evidence from the Costa Rican case ». 2011. http://www.die-gdi.de/en/others-publications/article/obstacles-to-citizen-participation-by-direct-democracy-in-latin-america-a-comparative-regional-analysis-of-legal-frameworks-and-evidence-from-the-costa-rican-case/.
Bridwell, Jana Marie. 2013. « Twitter, Texting, and Street Demonstrations: Assessing Social Media's Political Relevance for Citizen Empowerment ». SSRN Scholarly Paper ID 2299091. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2299091.
Broderick, Ryan, et Jules Darmanin. 2018. « The "Yellow Jackets" Riots In France Are What Happens When Facebook Gets Involved With Local News ». BuzzFeed News. 12 juin 2018. https://www.buzzfeednews.com/article/ryanhatesthis/france-paris-yellow-jackets-facebook.
Bruns, Axel. 2016. « User-Generated Content ». In *The International Encyclopedia of Communication Theory and Philosophy*, 1-5. American Cancer Society. https://doi.org/10.1002/9781118766804.wbiect085.
Bruns, Axel, et Jean Burgess. 2012. « Researching news discussion on Twitter: New methodologies ». *Journalism Studies* 13 (5-6): 801–814.
Bruns, Axel, Tim Highfield, et Jean Burgess. 2013. « The Arab Spring and Social Media Audiences: English and Arabic Twitter Users and Their Networks ». *American Behavioral Scientist* 57 (7): 871-98. https://doi.org/10.1177/0002764213479374.
Buschmann, Andy. 2018. « Introducing the *Myanmar Protest Event Dataset* Motivation, Methodology, and Research Prospects ». *Journal of Current Southeast Asian Affairs* 37 (2): 125-42. https://doi.org/10.1177/186810341803700205.
Camus, Jean-Yves. 2018. « Carnegie Council Presents Materials in French and English from Year-Long Research Project »,. 24 juillet 2018. https://www.carnegiecouncil.org/news/announcements/2018-07-24-carnegie-council-presents-materials-from-research-project-russian-soft-power-in-france.
CAPS/IRSEM. 2018. « Rapport conjoint CAPS/IRSEM - Les manipulations de l'information : Un défi pour nos démocraties (04.09.18) ». France Diplomatie : : Ministère de l'Europe et des Affaires étrangères. 2018. https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/manipulations-de-l-information/rapport-conjoint-caps-irsem-les-manipulations-de-l-information-un-defi-pour-nos/.
Carayon, Bernard, Philippe CADUC, Alain JUILLET, et Rémy PAUTRAT. 2003. « Intelligence économique ». *Compétitivité et Cohésion sociale (http://www. bcarayon-ie. com/)*.

http://bdc.aege.fr/public/Intelligence_economique_competitivite_et_cohesion_sociale_2003.pdf.
Cardon, Dominique. 2009. « Vertus démocratiques de l'Internet ». *Repéré à*. http://www.laviedesidees.fr/Vertus-democratiques-de-l-Internet.html.
Cardon, Dominique, et Fabien Granjon. 2013. *Médiactivistes*. 2e édition revue et augmentée. Paris: Les Presses de Sciences Po.
Casilli, Antonio a. 2010. *Les Liaisons numériques. Vers une nouvelle sociabilité?* Paris: Le Seuil.
Center for media litterracy. 2019. « Media Literacy: A Definition and More | Center for Media Literacy | Empowerment through Education | CML MediaLit Kit ™ | ». 2019. https://www.medialit.org/media-literacy-definition-and-more.
Centre interarmées de concepts, doctrines, et d'expérimentations. 2008. « Les opérations militaires d'influence ».
———. 2009. « Le renseignement d'intérêt militaire ».
———. 2010a. « Doctrine interarmées n°2, Renseignement df'intérêt militaire et contre-ingérence ». CICDE.
———. 2010b. « Knowledge Development ».
———. 2012. « Coopération civilo-militaire ».
———. 2013. « Réseaux sociaux, nature et conséquences pour les forces armées ».
Cha, Miriam, Gwon Youngjune, et H T Kung. 2015. « Twitter Geolocation and Regional Classification via Sparse Coding. », 582-85.
Chabanet, Didier, et Frédéric Royall. 2016. *From Silence to Protest: International Perspectives on Weakly Resourced Groups*. 1 edition. Farnham, Surrey, England ; Burlington, VT: Routledge.
Chen, James. 2018. « GAFAM Stocks ». Investopedia. 24 juillet 2018. https://www.investopedia.com/terms/g/gafam-stocks.asp.
Cheng, Zhiyuan, James Caverlee, et Kyumin Lee. 2010. « You Are Where You Tweet: A Content-Based Approach to Geo-Locating Twitter Users ». In *Proceedings of the 19th ACM International Conference on Information and Knowledge Management - CIKM '10*, 759. Toronto, ON, Canada: ACM Press. https://doi.org/10.1145/1871437.1871535.
Chi, Ed H., et Todd Mytkowicz. 2008. « Understanding the efficiency of social tagging systems using information theory ». In *Proceedings of the nineteenth ACM conference on Hypertext and hypermedia*, 81–88. HT '08. New York, NY, USA: ACM. https://doi.org/10.1145/1379092.1379110.
Chi, Ed, et Todd Mytkowicz. 2007. « Understanding Navigability of Social Tagging Systems ». In . http://www.viktoria.se/altchi/index.php?action=showsubmission&id=39.
Chicago Police Department. 2015. *Custom Notifications in Chicago*. *Special Order*. Vol. S10-05. http://webcache.googleusercontent.com/search?q=cache:G8q0WZPQ-CcJ:directives.chicagopolice.org/directives/data/a7a57bf0-1456faf9-bfa14-570a-a2deebf33c56ae59.html&hl=fr&gl=fr&strip=1&vwsrc=0.
Chierichetti, Flavio, Jon Kleinberg, Ravi Kumar, Mohammad Mahdian, et Sandeep Pandey. 2014. « Event Detection via Communication Pattern Analysis ». In *Eighth International AAAI Conference on Weblogs and Social Media*. http://www.aaai.org/ocs/index.php/ICWSM/ICWSM14/paper/view/8088.
CIAE. 2019. « Place de l'Emploi Public - CHEF DE MISSION/ADJOINT – EXPERT MONDES RUSSOPHONES ». 4 janvier 2019. https://place-ep-recrute.talent-soft.com/offre-de-emploi/imprimer-fiche-emploi-chef-de-mission-adjoint-expert-mondes-russophones_189870.aspx.
Cihon, Peter, et Taha Yasseri. 2016. « A biased review of biases in Twitter studies on political collective action ». *arXiv preprint arXiv:1605.04774*. https://arxiv.org/abs/1605.04774.

CNESCO. 2019. « Éducation aux médias et à l'actualité : comment les élèves s'informent-ils ? » *Le zoom du Cnesco*, février.
Commission du livre blanc sur la défense et la sécurité nationale, Commission du livre blanc sur la défense et la sécurité nationale, Commission du livre blanc sur la défense et la sécurité nationale, et Commission du livre blanc sur la défense et la sécurité nationale. 2013. *Livre blanc défense et sécurité nationale 2013*. Paris: la Documentation française : diff. Direction de l'information légale et administrative.
Commission Européenne. 2008. *Council Framework Decision 2008/913/JHA of 28 November 2008 on Combating Certain Forms and Expressions of Racism and Xenophobia by Means of Criminal Law*. *OJ L*. Vol. 328. http://data.europa.eu/eli/dec_framw/2008/913/oj/eng.
———. 2016. « The EU Code of conduct on countering illegal hate speech online | European Commission ». 30 juin 2016. https://ec.europa.eu/newsroom/document.cfm?doc_id=40573.
———. 2018a. « Final Report of the High Level Expert Group on Fake News and Online Disinformation ». Text. Digital Single Market - European Commission. 12 mars 2018. https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.
———. 2018b. « Lutter contre la désinformation en ligne: une approche européenne ». https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52018DC0236.
Confessore, Nicholas, Gabriel J. X. Dance, Rich Harris, et Mark Hansen. 2018. « The Follower Factory ». *The New York Times*, 27 janvier 2018, sect. Technology. https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html, https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html.
Cordeiro, Mário, et João Gama. 2016. « Online Social Networks Event Detection: A Survey ». In *Solving Large Scale Learning Tasks. Challenges and Algorithms*, édité par Stefan Michaelis, Nico Piatkowski, et Marco Stolpe, 9580:1-41. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-41706-6_1.
Corsaro, Nicholas, et Robin S. Engel. 2015. « Most Challenging of Contexts ». *Criminology & Public Policy* 14 (3): 471-505. https://doi.org/10.1111/1745-9133.12142.
Cosenza, Vincenzo. 2012. *Social Media ROI*. Apogeo Editore.
Curran, James, et David Hesmondhalgh, éd. 2019. *Media and Society*. 6th Revised edition edition. New York, NY: Bloomsbury Academic USA.
Dafoe, Allan, et Jason M. K. Lyall. 2015. « From Cell Phones to Conflict? Reflections on the Emerging ICT-Political Conflict Research Agenda ». In . https://doi.org/10.2139/ssrn.2409639.
Darczewska, Jolanta. 2014. « The Anatomy of Russian Information Warfare. The Crimean Operation, a Case Study ». OSW. 22 mai 2014. https://www.osw.waw.pl/en/publikacje/point-view/2014-05-22/anatomy-russian-information-warfare-crimean-operation-a-case-study.
Datta, Anupam, Shayak Sen, et Yair Zick. s. d. « Algorithmic Transparency via Quantitative Input Influence »:, 20.
Decourt, Remy. 2019. « SpaceX va lancer les 60 premiers satellites de la constellation Starlink ». 16 mai 2019. https://www.futura-sciences.com/sciences/actualites/spacex-spacex-va-lancer-60-premiers-satellites-constellation-starlink-76082/.
Délégation à l'Information et à la Communication de la Défense. 2012. « Guide de bon usage des médias sociaux ». www.defense.gouv.fr/guide-medias-sociaux/telecharger.pdf.
Délégations aux Affaires Stratégiques, ministère de la Défense. 2013. « Observatoire du monde cybernétique ».

Deuff, Olivier Le. 2012. « Littératies informationnelles, médiatiques et numériques : de la concurrence à la convergence ? » *Études de communication. langages, information, médiations*, no 38 (juin): 131-47. https://doi.org/10.4000/edc.3411.
Dhuicq, Nicolas. 2018. « (20) Nicolas DHUICQ sur Twitter : "#Alep #Syrie en 2017 nous avions reçu les roquettes des « rebelles modérés » de M. Fabius. La télévision montrait des munitions françaises, obus de mortiers et roquettes. Vidéo récente à voir pour l'origine des munitions trouvées par Russes https://t.co/V4lz9AioQl via @youtube" / Twitter ». Twitter. 17 avril 2018. https://twitter.com/NicolasDHUICQ/status/986151116231593984.
———. 2019. « (20) Nicolas DHUICQ sur Twitter : "#Syrie #Daesh pendant que certains crient victoire, ils oublient #Idlib qui reste le noeud central où sont concentrés tous les islamistes ! Aurons nous la même manipulation ? Terrorists in Syria's Idlib Plotting Chemical Weapons Provocation - Russian MoD https://t.co/qNxP2siLLe" / Twitter ». Twitter. 29 mars 2019. https://twitter.com/NicolasDHUICQ/status/1111709210574835714.
Diaz-Ortiz (Author), Biz Stone Claire. 2011. *Claire Diaz-Ortiz, Biz Stone'sTwitter for Good: Change the World One Tweet at a Time [Hardcover]2011*. Jossey-Bass.
Dimitrova, Antoaneta, Matthew Frear, Honorata Mazepus, Dimiter Toshkov, Maxim Boroda, Tatsiana Chulitskaya, Oleg Grytsenko, Igor Munteanu, Tatiana Parvan, et Ina Ramasheuskaya. s. d. « The Elements of Russia's Soft Power: Channels, Tools, and Actors Promoting Russian Influence in the Eastern Partnership Countries », 48.
Diuk, Nadia. 2013. « Youth as an Agent for Change: The next Generation in Ukraine ». Demokratizatsiya. 22 mars 2013. https://link.galegroup.com/apps/doc/A326130754/AONE?sid=lms.
Dixon, Andi, et William Isaac. s. d. « Why Big-Data Analysis of Police Activity Is Inherently Biased ». The Conversation. Consulté le 5 septembre 2019. http://theconversation.com/why-big-data-analysis-of-police-activity-is-inherently-biased-72640.
« Dublin Core Metadata Element Set ». 2012. 2012. http://dublincore.org/documents/dces/.
Duval, Alison. 2013. *Mobilisation du Tea Party, l'effet main invisible analyse du réseau internet d'un mouvement social conservateur*. Édité par Nonna Mayer et Institut d'études politiques (Paris). [S.l.]: [s.n.].
Eduscol. 2015. « Une éducation aux médias et à l'information renforcée ». https://cache.media.eduscol.education.fr/file/DP_rentree/35/1/2015_rentreescolaire_fiche_34_456351.pdf.
———. 2019. « Prévenir la radicalisation en milieu scolaire - Prévention de la radicalisation - Éduscol ». 2019. https://eduscol.education.fr/cid100811/prevention-radicalisation.html.
Egbert, Simon. 2019. « Predictive Policing and the Platformization of Police Work ». *Surveillance & Society* 17 (1/2): 83-88. https://doi.org/10.24908/ss.v17i1/2.12920.
Eltantawy, Nahed, et Julie B. Wiest. 2011. « The Arab spring| Social media in the Egyptian revolution: reconsidering resource mobilization theory ». *International Journal of Communication* 5: 18.
Europe1. 2018. « TF1 demande "moins de 20 millions d'euros" aux opérateurs ». *Europe 1*, 3 juin 2018. https://www.europe1.fr/medias-tele/tf1-demande-moins-de-20-millions-deuros-aux-operateurs-3592403.
Facebook. 2018. « Bringing People Closer Together | Facebook Newsroom ». 2018. https://newsroom.fb.com/news/2018/01/news-feed-fyi-bringing-people-closer-together/.

Farge, Arlette. 2002. « Penser et définir l'événement en histoire. Approche des situations et des acteurs sociaux ». *Terrain. Anthropologie & sciences humaines*, no 38 (mars): 67-78. https://doi.org/10.4000/terrain.1929.
Faris, David M. 2012. « Beyond 'Social Media Revolutions'. The Arab Spring and the Networked Revolt ». *Politique Étrangère* Spring Issue (1): 99-109.
Fillieule, Olivier. 2007. *On n'y voit rien: le recours aux sources de presse pour l'analyse des mobilisations protestataires*. Université de Lausanne, Institut d'études politiques et internationales.
Fillieule, Olivier, et Manuel Jiménez. 2003. « The Methodology of Protest Event Analysis and the Media Politics of Reporting Environmental Protest Events », 22.
Flichy, Patrice. 2008. « Internet et le débat démocratique ». *Réseaux*, no 4: 159–185.
Flintoff. 2014. « Are "Color Revolutions" A New Front In U.S.-Russia Tensions? » NPR.Org. 6 décembre 2014. https://www.npr.org/2014/06/12/321392873/are-color-revolutions-a-new-front-in-u-s-russia-tensions.
Fradin, Andrea. 2012. « La guerre des tuyaux ». 4 avril 2012. index.html.
France Info. 2019. « Tout comprendre à la bataille entre Free, Orange et BFMTV ». Franceinfo. 30 août 2019. https://www.francetvinfo.fr/economie/free/la-bataille-entre-bfmtv-free-et-orange-en-cinq-questions_3596783.html.
France24. 2018. « Des enfants qui font semblant de suffoquer : la dernière intox des pro-Assad ». Les Observateurs de France 24. 4 novembre 2018. https://observers.france24.com/fr/20180411-video-douma-fake-attaque-chimique-syrie.
Freedom House. 2013. « Ukraine ». 9 janvier 2013. https://freedomhouse.org/report/freedom-world/2013/ukraine.
Freeman, Linton C. 1978. « Centrality in Social Networks Conceptual Clarification ». *Social Networks* 1 (3): 215-39. https://doi.org/10.1016/0378-8733(78)90021-7.
Furnas, George W., Caterina Fake, Luis von Ahn, Joshua Schachter, Scott Golder, Kevin Fox, Marc Davis, Cameron Marlow, et Mor Naaman. 2006. « Why do tagging systems work? » In *CHI '06 Extended Abstracts on Human Factors in Computing Systems*, 36–39. CHI EA '06. New York, NY, USA: ACM. https://doi.org/10.1145/1125451.1125462.
Garrigues, Arnaud, et Olivier Kempf. 2012. « L'OTAN et la cyberdéfense ». *Sécurité globale* 19 (1): 133. https://doi.org/10.3917/secug.019.0133.
GDELT. 2019. « Data: Querying, Analyzing and Downloading: The GDELT Project ». 2019. https://www.gdeltproject.org/data.html#intro.
« GeoConcept géoptimise le Renseignement d'Intérêt Militaire ». 2012. http://www.geoconcept.com.
George, Éric. 2005. « Les usages sociaux d'internet au sein du mouvement altermondialiste entre promesses et réalités ». In *communication présentée au colloque Démocratie et dispositifs électroniques: regards sur la décision, la délibération et le militantisme organisé par le réseau DEL, Paris*.
Geraint, Evans. 2009. « Rethinking Military Intelligence Failure, Putting the Wheels Back on the Intelligence Cycle ». *Defense Studies*, 2009.
Gerasimov, Valeriy. 2013. « Ценность науки в предвидении | Еженедельник «Военно-промышленный курьер» ». *vpk-news.ru*, 26 février 2013. https://www.vpk-news.ru/articles/14632.
« Germany fines Facebook $2.3 million under hate speech law ». 2019. AP NEWS. 2 juillet 2019. https://apnews.com/7980a313e4a6483a939ae64989767a38.
Gerner, Deborah J., et Philip A. Schrodt. 1996. « The Kansas Event Data System: A Beginner's Guide with an Application to the Study of Media Fatigue in the Palestinian Intifada ». In .

Gerner, Deborah J., Philip A. Schrodt, Raja Abu-Jabr, et Omur Yilmaz. 2002. « Conflict and Mediation Event Observations (CAMEO): An Event Data Framework for a Post-Cold War World ». In *International Conflict Mediation*, 4:287-304. Routledge. https://doi.org/10.4324/9780203885130.pt5.

Gladstone, Rick. 2015. « Twitter Says It Suspended 10,000 ISIS-Linked Accounts in One Day ». *The New York Times*, 9 avril 2015. http://www.nytimes.com/2015/04/10/world/middleeast/twitter-says-it-suspended-10000-isis-linked-accounts-in-one-day.html.

Global Web Index. 2018. « Social : GlobalWebIndex's Flagship Report on the Latest Trends in Social Media ». H1. Global Web Index. http://files.r-trends.ru/reports/Social_Summary_Report_NEW.pdf.

Goffman, Erving. 1974. *Frame analysis: An essay on the organization of experience*. Frame analysis: An essay on the organization of experience. Cambridge, MA, US: Harvard University Press.

Golder, Scott A., et Bernardo A. Huberman. 2006. « Usage Patterns of Collaborative Tagging Systems ». *Journal of Information Science* 32 (2): 198-208. https://doi.org/10.1177/0165551506062337.

Golder, Scott, et Bernardo Huberman. 2005. « The Structure of Collaborative Tagging Systems ». http://arxiv.org/abs/cs.DL/0508082.

Gomza, Ivan. 2014. « Contentious Politics and Repertoire of Contention in Ukraine: The Case of Euromaidan », février. https://www.academia.edu/8499202/Contentious_Politics_and_Repertoire_of_Contention_in_Ukraine_The_Case_of_Euromaidan.

Goodwin, Jeff, James M. Jasper, et Jaswinder Khattra. 1999. « Caught in a Winding, Snarling Vine: The Structural Bias of Political Process Theory ». *Sociological Forum* 14 (1): 27-54.

Google. 30//11/12. « A little less than two years ago, when Internet access was cut off in Egypt, ... » 30//11/12. https://plus.google.com/+google/posts/dKiBsQq6nxw.

———. 2011. « Some Weekend Work That Will (Hopefully) Enable More Egyptians to Be Heard ». *Official Google Blog* (blog). janvier 2011. https://googleblog.blogspot.com/2011/01/some-weekend-work-that-will-hopefully.html.

———. 2013. « Introducing Project Loon: Balloon-Powered Internet Access ». *Official Google Blog* (blog). 2013. https://googleblog.blogspot.com/2013/06/introducing-project-loon.html.

Grande Ecole du numérique. 2015. « Tout savoir sur la création et le développement de la GEN ». La Grande Ecole du Numérique. 2015. https://www.grandeecolenumerique.fr/tout-savoir-sur-la-creation-et-le-developpement-de-la-gen.

Gruzd, Anatoliy, et Ksenia Tsyganova. 2015. « Information Wars and Online Activism During the 2013/2014 Crisis in Ukraine: Examining the Social Structures of Pro- and Anti-Maidan Groups ». *Policy & Internet* 7 (2): 121-58. https://doi.org/10.1002/poi3.91.

Gunitsky, Seva. 2015. « Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability ». *Perspectives on Politics* 13 (1): 42-54. https://doi.org/10.1017/S1537592714003120.

Hamdi-Kidar, Linda. 2013. « Co-création marketing de produit avec les consommateurs: quelle(s) cible(s) choisir ? » Thèse de doctorat, Toulouse, France: École Doctorale Sciences de Gestion.

Hanna, Alex. 2017. « MPEDS: Automating the Generation of Protest Event Data », janvier. https://doi.org/10.31235/osf.io/xuqmv.

Hecker, Marc. 2014. « Le tsunami numérique. gérer les catastrophes naturelles à l'heure des réseaux sociaux ». *Etudes 2014/7*, juillet 2014.
Hecker, Marc, Nicolas Vanbremeersch, Marguerite de Durand, et Thibault Souchet. 2012. « Nature et conséquence des réseaux sociaux pour les forces armées ». IFRI, SPINTANK.
Hérodote. 1850. *Histoire d'Hérodote*. Paris: Charpentier.
Hirose, Kentaro, Kosuke Imai, et Jason Lyall. 2017. « Can Civilian Attitudes Predict Insurgent Violence? Ideology and Insurgent Tactical Choice in Civil War ». *Journal of Peace Research* 54 (1): 47-63. https://doi.org/10.1177/0022343316675909.
Hon, Linda. 2016. « Social Media Framing Within the Million Hoodies Movement for Justice ». *Institute for Public Relations* (blog). 12 janvier 2016. https://instituteforpr.org/social-media-framing-within-the-million-hoodies-movement-for-justice/.
Hooton, Christopher. 2014. « Dear Subscriber, You Are Registered as a Participant in a Mass Disturbance ». *The Independent*, 22 janvier 2014, The Independent édition. http://www.independent.co.uk/news/world/europe/ukraine-protests-demonstrators-in-kiev-receive-disturbing-mass-text-9077327.html.
Horn, Jessica. 2013. *Gender and social movements overview report*. IDS.
Horton, Woody. 2007. « Introduction à la maîtrise de l'information: une explication, en termes simples et sans jargon technique, de ce que l'on entend par maîtrise de l'information, à l'intention des responsables des pol... - UNESCO Bibliothèque Numérique ». Unesco. https://unesdoc.unesco.org/ark:/48223/pf0000157020_fre.
Howells, Richard. 2001. « Media, Education and Democracy ». *European Review* 9 (2): 159-68. https://doi.org/10.1017/S1062798701000151.
Hua, Ting, Yue Ning, Feng Chen, Chang-Tien Lu, et Naren Ramakrishnan. 2016. « Topical Analysis of Interactions Between News and Social Media ». In *Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence*, 2964–2971. AAAI'16. AAAI Press. http://dl.acm.org/citation.cfm?id=3016100.3016317.
Huang, Qunying, et Yu Xiao. 2015. « Geographic Situational Awareness: Mining Tweets for Disaster Preparedness, Emergency Response, Impact, and Recovery ». *ISPRS International Journal of Geo-Information* 4 (3): 1549-68. https://doi.org/10.3390/ijgi4031549.
Hulnick, Arthur S. 2006. « What's wrong with the Intelligence Cycle ». *Intelligence and National Security* 21 (6): 959-79. https://doi.org/10.1080/02684520601046291.
Huspeni, Andrea. 2017. « Why Mark Zuckerberg Runs 10,000 Facebook Versions a Day ». Entrepreneur. 24 mai 2017. https://www.entrepreneur.com/article/294242.
Hutter, Swen. 2014. « Protest Event Analysis and Its Offspring ». In , 335-67. https://doi.org/10.1093/acprof:oso/9780198719571.003.0014.
I4ADA. 2018. « I4ADA – Institute for Accountability and Internet Democracy ». 6 janvier 2018. https://i4ada.org/.
Internet Association. 2019. « Content Moderation ». Internet Association. 2019. https://internetassociation.org/positions/content-moderation/.
Internet Governance Forum. 2019. « About the IGF ». Text. Internet Governance Forum. 2019. https://www.intgovforum.org/multilingual/tags/about.
Internet Live Stats. 2019. « Total Number of Websites - Internet Live Stats ». 2019. https://www.internetlivestats.com/total-number-of-websites/.
Internet World Stats. 2019. « Internet 50 Countries with Highest Penetration Rates ». 2019. http://www.internetworldstats.com/top25.htm.
Interpol. 2018. « Open calls for tender ». 2018. https://www.interpol.int/fr/Qui-nous-sommes/Achats/Appels-d-offres-ouverts.
IPI. 2011. « The Role of Social Media in Promoting Democratization and Human Rights: Prospects and Challenges ». In . International Peace Institute.

https://www.ipinst.org/wp-content/uploads/2011/09/pdfs_transcript-socialmedia-sept2011.pdf.
Irondelle, Bastien, et Amélie Malissard. s. d. « ETUDIER LE RENSEIGNEMENT ÉTAT DE L'ART ET PERSPECTIVES DE RECHERCHE », 266.
Jacobs, Andreas, et Guillaume Lasconjarias. 2015. « NATO'S Hybrid Flanks, handling unconventional warfare in the south and the east. » Research paper 112. Rome: Nato Defense COllege, Research Division.
Jasper, James M. 1997. *The Art of Moral Protest: Culture, Biography, and Creativity in Social Movements*. University of Chicago Press.
Jenkins, J. Craig. 1983. « Resource Mobilization Theory and the Study of Social Movements ». *Annual Review of Sociology* 9: 527-53.
Jenkins, J. Craig, et Thomas V. Maher. 2016. « What Should We Do about Source Selection in Event Data? Challenges, Progress, and Possible Solutions ». *International Journal of Sociology* 46 (1): 42-57. https://doi.org/10.1080/00207659.2016.1130419.
Jenkins, Joseph C., et Charles Perrow. 1977. « Insurgency of the Powerless: Farm Worker Movements (1946-1972). » In . https://doi.org/10.2307/2094604.
Joh, Elizabeth E. s. d. « Feeding the Machine: Policing, Crime Data, & Algorithms » 26: 17.
Johnson, Loch K. 2009. *Handbook of Intelligence Studies*. London; New York: Routledge.
Json.org. 2019. « JSON ». 2019. https://www.json.org/json-fr.html.
Jurgens, David, Tyler Finethy, James McCorriston, Yi Tian Xu, et Derek Ruths. 2015. « Geolocation Prediction in Twitter Using Social Networks: A Critical Analysis and Review of Current Practice ». In *Ninth International AAAI Conference on Web and Social Media*. http://www.aaai.org/ocs/index.php/ICWSM/ICWSM15/paper/view/10584.
Kalogiros, Costas. 2012. « A taxonomy for Future Internet stakeholders - SESERV ». 31 octobre 2012. http://www.seserv.org/fise-conversation/ataxonomyforfutureinternetstakeholders.
Karlsen, Geir Hågen. 2019. « Divide and Rule: Ten Lessons about Russian Political Influence Activities in Europe ». *Palgrave Communications* 5 (1): 1-14. https://doi.org/10.1057/s41599-019-0227-8.
Kelly, Sanja, Mai Truong, Madeline Earp, Laura Reed, Adrian Shahbaz, et Ashley greco-Stoner. 2013. « Freedom on the Net 2013 ». Freedom House. http://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf.
Kibanov, Mark, Gerd Stumme, Imaduddin Amin, et Jong Gun Lee. 2017. « Mining Social Media to Inform Peatland Fire and Haze Disaster Management ». *Social Network Analysis and Mining* 7 (1). https://doi.org/10.1007/s13278-017-0446-1.
Knobel, Marc. 2012. *L'internet de la haine: racistes, antisémites, néonazis, intégristes, islamistes, terroristes et homophobes à l'assaut du web*. Édité par J'accuse ! Paris, France: Berg international, DL 2012.
Koch, Olivier. 2018. « Les données de la guerre. Big Data et algorithmes à usage militaire ». *Les Enjeux de l'information et de la communication* N° 19/2 (2): 113-23.
———. 2019. « Portrait de l'intellectuel en soldat ». *Le Monde diplomatique* N° 780 (3): 12-12.
koopmans, Ruud, et Dieter Rucht. 2002. « Protest Event Analysis ». In *Methods of Social Mmovement Research*, University of Minnesota Press.
Kousis, Maria, Marco Giugni, et Christian Lahusen. 2018. « Action Organization Analysis: Extending Protest Event Analysis Using Hubs-Retrieved Websites ». *American Behavioral Scientist* 62 (6): 739-57. https://doi.org/10.1177/0002764218768846.

Kriesi, Hanspeter, Ruud Koopmans, Jain Willem Duyvendak, et Marco Giugni. 1995. « New Social Movements in Western Europe: A Comparative Analysis ». https://archive-ouverte.unige.ch/unige:92400.

Kumar, Ravi, Jasmine Novak, et Andrew Tomkins. 2006. « Structure and evolution of online social networks ». In *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining*, 611–617. KDD '06. New York, NY, USA: ACM. https://doi.org/10.1145/1150402.1150476.

Kwasniewski, Nicolai. s. d. « European Satellites: How Islamic State Takes Its Terror To the Web - SPIEGEL ONLINE - International ». SPIEGEL ONLINE. Consulté le 16 avril 2017. http://www.spiegel.de/international/world/islamic-state-uses-satellite-internet-to-spread-message-a-1066190.html.

Lambert, Frederic. 2019. « L'éducation aux médias en Europe : controverses, défis et perspectives ». In *Euromeduc*. https://eduscol.education.fr/numerique/dossier/competences/education-aux-medias/bibliographie-webographie/colloques-seminaires/l-education-aux-medias-en-europe-controverses-defis-et-perspectives.

Lamer, Wiebke. 2012. « Twitter and Tyrants: New Media and its Effects on Sovereignty in the Middle East ». Arab Media & Society. 8 juillet 2012. http://www.arabmediasociety.com/?article=798.

Larousse, Éditions. 2019. « Définitions : mobilisation - Dictionnaire de français Larousse ». 2019. https://www.larousse.fr/dictionnaires/francais/mobilisation/51883.

Laruelle, Marlene. s. d. « Le "soft power" russe en France: La para-diplomatie culturelle et d'affaires », 18.

Lawrence, Steve, et C. Lee Giles. 1999. « Accessibility of information on the web ». *Nature* 400 (6740): 107–107.

Leetaru, Kalev, et Philip A. Schrodt. 2013. « GDELT: Global data on events, location, and tone ». *ISA Annual Convention*.

Lehrner, Amy, et Nicole E. Allen. 2008. « Social Change Movements and the Struggle over Meaning-Making: A Case Study of Domestic Violence Narratives ». *American Journal of Community Psychology* 42 (3-4): 220-34. https://doi.org/10.1007/s10464-008-9199-3.

Letort, Delphine. 2014. « Les documentaires politiques de Robert Greenwald: définir des nouvelles pratiques militantes à l'ère d'Internet ». *Revue LISA/LISA e-journal. Littératures, Histoire des Idées, Images, Sociétés du Monde Anglophone–Literature, History of Ideas, Images and Societies of the English-speaking World* 12 (1).

Lewis, Jenny, Ida Groth, Sebastian Kjeldtoft, Sebastian Lykke, et Toke nielsen. 2012. « Internet Governance - Balancing Freedom & Security Online ».

Li, Abner. 2015. « Report: Google X Absorbing Robotics Division and Titan Drone Project as Alphabet Re-Org Continues ». *9to5Google* (blog). 19 décembre 2015. https://9to5google.com/2015/12/18/google-x-robotics-titan-drone/.

Lichtenberg, Judith, éd. 1990. *Democracy and the Mass Media: A Collection of Essays*. First Edition edition. Cambridge ; New York: Cambridge University Press.

Livingston, Steven, et Gregor Walter-Drop. 2012. « Information and communication technologies in areas of limited statehood ». http://www.diss.fu-berlin.de/docs/receive/FUDOCS_document_000000015245.

Loosen, Wiebke, et Jan-Hinrik Schmidt. 2012. « (re-)discovering the Audience ». *Information, Communication & Society* 15 (6): 867-87. https://doi.org/10.1080/1369118X.2012.665467.

Lorenzini, Jasmine, Peter Makarov, Hanspeter Kriesi, et Bruno Wueest. 2016. « Towards a Dataset of Automatically Coded Protest Events from English-Language Newswire Documents », 35.
Lotan, Gilad, Erhardt Graeff, Mike Ananny, Devin Gaffney, Ian Pearce, et Danah Boyd. 2011. « The Arab Spring| The Revolutions Were Tweeted: Information Flows during the 2011 Tunisian and Egyptian Revolutions ». *International Journal of Communication* 5 (0): 31.
Maillard, Clément de. 2014. « La France et le renseignement criminel : entre volonté et réalité, une ambition à écrire. » *sécurité et stratégie* 17 (revue des directeurs sécurité d'entreprises).
Major, Claudia, et Christian Mölling. s. d. « Entre la crise et la responsabilité : un premier bilan de la nouvelle politique de défense allemande ». Institut français des relations internationales. Consulté le 20 septembre 2019. https://www.ifri.org/fr/publications/enotes/notes-cerfa/entre-crise-responsabilite-un-premier-bilan-de-nouvelle-politique-de.
Makarov, Peter, Jasmine Lorenzini, et Hanspeter Kriesi. 2016. « Constructing an Annotated Corpus for Protest Event Mining ». In *Proceedings of the First Workshop on NLP and Computational Social Science*, 102–107. Austin, Texas: Association for Computational Linguistics. https://doi.org/10.18653/v1/W16-5613.
Manise, JeanLuc. 2012. « De l'activisme numérique au militantisme de terrain ».
Marlow, Cameron, Mor Naaman, Danah Boyd, et Marc Davis. 2006. « HT06, tagging paper, taxonomy, Flickr, academic article, to read ». In , 31-40. ACM. https://doi.org/10.1145/1149941.1149949.
Marsden, Christopher. 2017. *Network Neutrality: From Policy to Law to Regulation*. Manchester University Press. https://doi.org/10.26530/OAPEN_622853.
Martens, Pascal. 2016. « PREDICTIVE POLICING TENSION BETWEEN ANALYTICS AND INTUITION », juin, 12.
Maton, Kenneth I. 2008. « Empowering Community Settings: Agents of Individual Development, Community Betterment, and Positive Social Change ». *American Journal of Community Psychology* 41 (1-2): 4-21. https://doi.org/10.1007/s10464-007-9148-6.
McAdam, Doug, et David A. Snow, éd. 1997. *Social Movements: Readings on Their Emergence, Mobilization, and Dynamics*. 1st edition. New York: Oxford University Press.
McAdam, Doug, Sidney Tarrow, et Charles Tilly. 2001. *Dynamics of Contention*. Cambridge ; New York: Cambridge University Press.
McCarthy, John D., et Mayer N. Zald. 1977. « Resource Mobilization and Social Movements: A Partial Theory ». *American Journal of Sociology* 82 (6): 1212-41.
Meijer, Albert, et Martijn Wessels. 2019. « Predictive Policing: Review of Benefits and Drawbacks ». *International Journal of Public Administration* 42 (12): 1031-39. https://doi.org/10.1080/01900692.2019.1575664.
Meister, Stefan. 2016. « Isolation and Propaganda: The Roots and Instruments of Russia's Disinformation Campaign ». *The German Marshall Fund of the United States* Policy Paper (avril). http://www.gmfus.org/publications/isolation-and-propaganda-roots-and-instruments-russia%E2%80%99s-disinformation-campaign.
Menold, Natalja, Johann Schaible, Theoni Stathopoulou, et Cornelia Zuell. 2018. « Development of a Methodology to Measure Media Context in the European Social Survey », 34.
Metaxas, Panagiotis, Eni Mustafaraj, Kily Wong, Laura Zeng, Megan O'Keefe, et Samantha Finn. 2015. « What Do Retweets Indicate? Results from User Survey and Meta-Review of Research ». In *Ninth International AAAI Conference on Web and Social Media*. http://www.aaai.org/ocs/index.php/ICWSM/ICWSM15/paper/view/10555.

Meyer, David S., et Debra C. Minkoff. 2004. « Conceptualizing Political Opportunity ». *Social Forces* 82 (4): 1457-92. https://doi.org/10.1353/sof.2004.0082.
Michel, Casey. 2017. « Opinion | How the Russians Pretended to Be Texans — and Texans Believed Them ». *Washington Post*, 17 octobre 2017, sect. DemocracyPost Opinion Opinion A column or article in the Opinions section (in print, this is known as the Editorial Pages). https://www.washingtonpost.com/news/democracy-post/wp/2017/10/17/how-the-russians-pretended-to-be-texans-and-texans-believed-them/.
Minas, Harry. 2010. « CAN THE OPEN SOURCE INTELLIGENCE EMERGE AS AN INDISPENSABLE DISCIPLINE FOR THE INTELLIGENCE COMMUNITY IN THE 21st CENTURY? » Research institute for european and american studies.
Ministère de la Culture. 2019. « Lancement d'un appel à projets national sur l'éducation aux médias et à l'information - Ministère de la Culture ». 2019. http://www.culture.gouv.fr/Presse/Communiques-de-presse/Lancement-d-un-appel-a-projets-national-sur-l-education-aux-medias-et-a-l-information.
Ministère de la Défense. 2003. *INSTRUCTION INTERARMEES SUR LE RENSEIGNEMENT D'INTERET MILITAIRE*. *PIA 02-200*. Vol. n° 1076/DEF/EMA/EMP.1/NP.
———. 2010. « Connaître et anticiper ». 7 décembre 2010. https://www.defense.gouv.fr/air/defis/fonctions-strategiques/connaitre-et-anticiper/connaitre-et-anticiper.
———. 2018a. « Projet de loi de programmation militaire pour les années 2019 à 2025 - rapport annexé ». ARMX1800503L/Bleue-1.
———. 2018b. « Big data et IA : la DGA présente le projet Artemis ». defense.gouv.fr. 10 août 2018. https://www.defense.gouv.fr/dga/actualite/big-data-et-ia-la-dga-presente-le-projet-artemis.
Ministère de la Défense, DGRIS. 2017. « Revue stratégique de défense et de sécurité nationale 2017 ». https://www.defense.gouv.fr/dgris/presentation/evenements-archives/revue-strategique-de-defense-et-de-securite-nationale-2017.
Mislove, Alan, Bimal Viswanath, Krishna P. Gummadi, et Peter Druschel. 2010. « You Are Who You Know: Inferring User Profiles in Online Social Networks ». In *Proceedings of the Third ACM International Conference on Web Search and Data Mining*, 251–260. WSDM '10. New York, NY, USA: ACM. https://doi.org/10.1145/1718487.1718519.
Mongin, Dominique. 2012. *Les cyberattaques, armes de guerre en temps de paix*. 1. Editions Esprit. http://www.cairn.info/revue-esprit-2013-1-page-32.htm.
Montabert, Stéphane. 2017. « Monde : Le blog de Stéphane Montabert ». Le blog de Stéphane Montabert. 4 novembre 2017. http://stephanemontabert.blog.24heures.ch/archives/category/monde/index-9.html/.
Morin, Edgar. 1976. « Pour une crisologie ». *Communications* 25 (1): 149-63. https://doi.org/10.3406/comm.1976.1388.
Morstatter, Fred, Nichola Lubold, Heather Pon-Barry, Jürgen Pfeffer, et Huan Liu. 2014. « Finding Eyewitness Tweets During Crises ». In *Proceedings of the ACL 2014 Workshop on Language Technologies and Computational Social Science*, 23-27. Baltimore, MD, USA: Association for Computational Linguistics. https://doi.org/10.3115/v1/W14-2509.
Morstatter, Fred, Jürgen Pfeffer, Huan Liu, et Kathleen M. Carley. 2013. « Is the Sample Good Enough? Comparing Data from Twitter's Streaming API with Twitter's Firehose. » In .
Moser, Kurt. 2012. « PoolParty Thesaurus, Wordpress plugin ».
Moses, Lyria Bennett, et Janet Chan. 2018. « Algorithmic prediction in policing: assumptions, evaluation, and accountability ». *Policing and Society* 28 (7): 806-22. https://doi.org/10.1080/10439463.2016.1253695.

Mughan, Anthony, et Richard Gunther. 2000. « The Media in Democratic and Nondemocratic Regimes: A Multilevel Perspective ». Democracy and the Media: A Comparative Perspective. juillet 2000. https://doi.org/10.1017/CBO9781139175289.001.
Nasirifard, Peyman, Sheila Kinsella, Krystian Samp, et Stefan Decker. 2010. « Social People-Tagging vs. Social Bookmark-Tagging ». In *Knowledge Engineering and Management by the Masses*, édité par Philipp Cimiano et H. Sofia Pinto, 150-62. Lecture Notes in Computer Science 6317. Springer Berlin Heidelberg. http://link.springer.com/chapter/10.1007/978-3-642-16438-5_11.
National Public Radio. 2014. « Are "Color Revolutions" A New Front In U.S.-Russia Tensions? » NPR.Org. 6 décembre 2014. https://www.npr.org/2014/06/12/321392873/are-color-revolutions-a-new-front-in-u-s-russia-tensions.
Ning, Yue, Rongrong Tao, Chandan K. Reddy, Huzefa Rangwala, James C. Starz, et Naren Ramakrishnan. 2018. « STAPLE: Spatio-Temporal Precursor Learning for Event Forecasting ». In *SDM*. https://doi.org/10.1137/1.9781611975321.17.
Nora, Pierre. 1972. « L'événement monstre ». *Communications* 18 (1): 162-72. https://doi.org/10.3406/comm.1972.1272.
Nye, Joseph. 2014. « The Regime Complex for Managing Global Cyber Activities ». PAPER SERIES 1. Global Commission on Internet Governance. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.
O'Brien, Sean P. 2010. « Crisis Early Warning and Decision Support: Contemporary Approaches and Thoughts on Future Research ». *International Studies Review* 12 (1): 87-104.
Oleinik, Anton, et Olga Strelkova. 2015. « The relocation of a repertoire of collective action: Maidan 2013 ». *European Journal of Cultural and Political Sociology* 2 (2): 146-71. https://doi.org/10.1080/23254823.2015.1110291.
Olivier. 2018. « Facebook lancera son premier satellite Athena en 2019 ». *Journal du Geek* (blog). 29 juillet 2018. https://www.journaldugeek.com/2018/07/29/facebook-lancera-premier-satellite-athena-2019/.
Onuch, Olga. 2015. « 'Facebook Helped Me Do It': Understanding the EuroMaidan Protester 'Tool-Kit' ». *Studies in Ethnicity and Nationalism* 15 (1): 170-84. https://doi.org/10.1111/sena.12129.
Organisation des Nations Unies. 2011. « Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development ». Koninklijke Brill NV. https://doi.org/10.1163/2210-7975_HRD-9970-2016149.
———. 2016. « La promotion, la protection et l'exercice des droits de l'homme sur Internet ». A/HRC/32/L.20. Conseil des droits de l'homme. http://digitallibrary.un.org/record/845728/files/A_HRC_32_L-20-FR.pdf.
Organisation des Nations Unies, et High-level Panel on Digital Cooperation. 2019. « The Age of Digital Interdependence - Report of the UN Secretary-General's High-level Panel on Digital Cooperation ». Itu.int. https://www.itu.int/md/S19-CWGWSIS34-INF-0001.
Organisation für Sicherheit und Zusammenarbeit in Europa, Transnational Threats Department, Organisation für Sicherheit und Zusammenarbeit in Europa, et Strategic Police Matters Unit. 2017. *OSCE Guidebook Intelligence-Led Policing*. http://www.osce.org/chairmanship/327476?download=true.
OTAN. 2001. « NATO OSINT Handbook ».
———. 2002a. « NATO Intelligence exploitation of the Internet ».
———. 2002b. « NATO OSINT Reader ».
———. 2009. « Glossaire OTAN de termes et de définitions ».

———. 2015. « Keynote Speech by NATO Secretary General Jens Stoltenberg at the Opening of the NATO Transformation Seminar ». NATO. 19 mai 2015. http://www.nato.int/cps/en/natohq/opinions_118435.htm.
Parlement Européen. 2016a. « DIRECTIVE (UE) 2016/ 680 DU PARLEMENT EUROPÉEN ET DU CONSEIL - du 2 7 avril 2016 - relative à la protection des personnes physiques à l'égard du traite ment des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/ 977/ JAI du Conseil », avril, 43.
———. 2016b. « RAPPORT sur la communication stratégique de l'Union visant à contrer la propagande dirigée contre elle par des tiers ». http://www.europarl.europa.eu/doceo/document/A-8-2016-0290_FR.html.
Pearce, Katy E. 2014. « Two Can Play at that Game: Social Media Opportunities in Azerbaijan for Government and Opposition ». a 2014. https://www.academia.edu/5833149/Two_Can_Play_at_that_Game_Social_Media_Opportunities_in_Azerbaijan_for_Government_and_Opposition.
———. 2015. « The Best Defense Is a Good Offense: The Role of Social Media in the Current Crackdown in Azerbaijan », no 70: 4.
Pearce, Katy E., et Adnan Hajizada. 2014. « No Laughing Matter Humor as a Means of Dissent in the Digital Era: The Case of Authoritarian Azerbaijan ». *Demokratizatsiya* 22 (1): 67–85.
Pellet, Alain, Anne-Thida Norodom, et Société française pour le droit international. Colloque. 2014. *Internet et le droit international*. Paris, France: Pedone, DL 2014.
Pew Research Center. 2014. « Ukrainians Want Unity Amid Worries about Political Leadership and Ethnic Conflict ». *Pew Research Center's Global Attitudes Project* (blog). 5 août 2014. https://www.pewresearch.org/global/2014/05/08/chapter-1-ukraine-desire-for-unity-amid-worries-about-political-leadership-ethnic-conflict/.
Phythian, Mark. 2013. *Understanding the Intelligence Cycle*. Londres: Routledge.
Pilster, Ulrich, et Tobias Böhmelt. 2014. « Predicting the Duration of the Syrian Insurgency ». *Research & Politics* 1 (2): 2053168014544586. https://doi.org/10.1177/2053168014544586.
Pleming, Sue. 2009. « U.S. State Department Speaks to Twitter over Iran ». *Reuters*, 16 juin 2009. https://www.reuters.com/article/us-iran-election-twitter-usa-idUSWBT01137420090616.
« point Godwin — Wiktionnaire ». 2019. In *Wiktionnaire*. https://fr.wiktionary.org/wiki/point_Godwin.
Police allemande. 2019. « Ausschreibungen und Bekanntmachungen ». 2019. http://www.icc-hofmann.de/cgi-bin/docorder?FM_ND=20190815125322839 68.
Police Blege. 2018. « i-Police: la police va prévoir la criminalité grâce à des algorithmes ». Communes, régions, Belgique, monde, sports – Toute l'actu 24h/24 sur Lavenir.net. 2018. https://www.lavenir.net/cnt/dmf20180830_01216050/i-police-la-police-va-prevoir-la-criminalite-grace-a-des-algorithmes.
Posadas, Brianna. 2017. « How Strategic Is Chicago's "Strategic Subjects List"? Upturn Investigates. » Medium. 26 juin 2017. https://medium.com/equal-future/how-strategic-is-chicagos-strategic-subjects-list-upturn-investigates-9e5b4b235a7c.
Predpol. 2019. « PredPol Mission | About Us | Aiming to Reduce Victimization Keep Communities Safer ». *PredPol* (blog). 2019. https://www.predpol.com/about/.

Price, Brian. 2017. « Human Terrain at the Crossroads ». National Defense University Press. 2017. http://ndupress.ndu.edu/Media/News/News-Article-View/Article/1325979/human-terrain-at-the-crossroads/.
Quintarelli, Emanuele. 2005. *Folksonomies: power to the people*. http://www-dimat.unipv.it/biblio/isko/doc/folksonomies.htm.
Rahimi, Afshin, Trevor Cohn, et Timothy Baldwin. 2015. « Twitter User Geolocation Using a Unified Text and Network Prediction Model ». In *Proceedings of the 53rd Annual Meeting of the Association for Computational Linguistics and the 7th International Joint Conference on Natural Language Processing (Volume 2: Short Papers)*, 630-36. Beijing, China: Association for Computational Linguistics. https://doi.org/10.3115/v1/P15-2104.
Rashed, Fawaz. 2011. « "We Use Facebook to Schedule the Protests, Twitter to Coordinate, and YouTube to Tell the World." #egypt #jan25 ». Tweet. *@FawazRashed* (blog). 18 mars 2011. https://twitter.com/FawazRashed/status/48882406010257408?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E48882406010257408&ref_url=https%3A%2F%2Fwww.theguardian.com%2Fworld%2F2016%2Fjan%2F25%2Fegypt-5-years-on-was-it-ever-a-social-media-revolution.
Rastier, François. 1989. *Sens et textualité*. Paris: Hachette.
Rattenbury, Tye, Nathaniel Good, et Mor Naaman. 2007. « Towards automatic extraction of event and place semantics from flickr tags ». In *Proceedings of the 30th annual international ACM SIGIR conference on Research and development in information retrieval*, 103–110. SIGIR '07. New York, NY, USA: ACM. https://doi.org/10.1145/1277741.1277762.
Rauniar, Rupak, Greg Rawski, Yang Jei, et Ben Johnson. 2014. « Technology acceptance model (TAM) and social media usage: An empirical study on Facebook ». *Journal of Enterprise Information Management* 27 (février). https://doi.org/10.1108/JEIM-04-2012-0011.
Rawat, Rakesh. 2010. « User behaviour modelling in a multi-dimensional environment for personalization and recommendation ». http://eprints.qut.edu.au/48135/.
Raymond, Mark, et Laura DeNardis. 2015. « Multistakeholderism: Anatomy of an Inchoate Global Institution ». *International Theory* 7 (3): 572-616. https://doi.org/10.1017/S1752971915000081.
Raza, Arslan Ali, Asad Habib, Jawad Ashraf, et Muhammad Javed. 2019. « Semantic Orientation Based Decision Making Framework for Big Data Analysis of Sporadic News Events ». *Journal of Grid Computing* 17 (2): 367-83. https://doi.org/10.1007/s10723-018-9466-y.
RDFS. 2010. « SIOC Core Ontology Specification ». 25 mars 2010. http://rdfs.org/sioc/spec/.
Regard sur le numérique. 2015. « La cyberguerre ? un abus de langage : Interview du Vice-Amiral Coustillière, officier général à la Cyberdéfense ». 22 janvier 2015. //archives.rsln.fr/fil/la-cyberguerre-un-abus-de-langage-interview-du-vice-amiral-coustilliere-officier-general-a-la-cyberdefense/.
Réseau Voltaire. 2013. « Gaz sarin en Syrie : nouvelle opération de propagande ». Réseau Voltaire. 22 août 2013. https://www.voltairenet.org/article179893.html.
Reuters. 2014. « Timeline: Political Crisis in Ukraine and Russia's Occupation of Crimea ». *Reuters*, 8 mars 2014. https://www.reuters.com/article/us-ukraine-crisis-timeline-idUSBREA270PO20140308.
Ricœur, Paul. 1992. « Le retour de l'Événement ». *Mélanges de l'école française de Rome* 104 (1): 29-35. https://doi.org/10.3406/mefr.1992.4195.
Ricordel, Pierre-Michel, Yves Demazeau, Guillaume Chicoisne, et Sylvie Pesty. 1998. « Outils et pistes pour la pratique du dialogisme entre agents ». *Journées Francophones sur l'Intelligence Artificielle Distribuée et les Systèmes Multi-Agents*, 164-76.

Riemer, Kai, Stephan Diederich, Alexander Richter, et Paul Scifleet. 2011. « Tweet Talking-Exploring The Nature Of Microblogging at Capgemini Yammer ». http://prijipati.library.usyd.edu.au/handle/2123/7226.
Rouzé, Vincent, Jacob Matthews, et Jérémy Vachet. 2014. *La Culture par les foules ?: Le crowdfunding et le crowdsourcing en question*. 1re éd. MkF Éditions.
RSF. 2016. « Kit de sécurité numérique | Reporters sans frontières ». RSF. 18 février 2016. https://rsf.org/fr/kit-de-securite-numerique.
RTBF. 2019. « La Belgique et la France en train de préparer une attaque chimique en Syrie? La Défense dénonce une fake news ». RTBF Info. 30 mars 2019. https://www.rtbf.be/info/belgique/detail_la-belgique-et-la-france-en-train-de-preparer-une-attaque-chimique-en-syrie-la-defense-denonce-une-fake-news?id=10183839.
Russia Today. 2016. « '6 Killed in Airstrike' on Village in Aleppo Province, Belgium Denies Involvement ». RT International. 19 octobre 2016. https://www.rt.com/news/363228-aleppo-airstrike-belgian-jets/.
———. 2019. « Pour Moscou, les renseignements français prépareraient une provocation à l'arme chimique en Syrie ». RT en Français. 29 mars 2019. https://francais.rt.com/international/60516-pour-moscou-renseignements-francais-prepareraient-provocation-arme-chimique-syrie.
Ruths, Derek, et Jürgen Pfeffer. 2014. « Social media for large studies of behavior ». *Science* 346 (6213): 1063–1064.
Sabah, Gérard. 1997. « Le point sur le sens ». 1997. http://perso.limsi.fr/Individu/gs/textes/ATALA-14.12.96/LePointSurLeSens.html.
Sadowsky, George. 2011. The I* Organizations and their Contribution to Development Global Internet Policy Initiative » FoIGFA Workshop on Internet Governance for Development in Nairobi, Kenya. http://friendsoftheigf.org/transcript/47.
Safranek, Rita. 2012. « The emerging role of social media in political and regime change ». *ProQuest Discovery Guides*. http://www.databank.com.lb/docs/The%20Emerging%20Role%20of%20Social%20Media%20in%20Political%20and%20Regime%20Change%20-2012.pdf.
Satsentinel. 2013. « Satellite Sentinel Project ». 2013. http://www.satsentinel.org/.
Schaurer, Florian, et Jan Störger. 2011. « The evolution of OSINT ». *Journal of US Intelligence Studies*, 2011.
Scheide, Carmen, et Ulrich Schmidt. 2014. « THE EUROMAIDAN IN UKRAINE November 2013 till February 2014 ». *Euxeinos. Governance and Culture in the Black Sea Region* 01. https://www.hsozkult.de/journal/id/zeitschriftenausgaben-8155?language=en.
Schinas, Manos, Symeon Papadopoulos, Yiannis Kompatsiaris, et Pericles Mitkas. 2018. « Event Detection and Retrieval on Social Media ». *arXiv:1807.03675 [cs]*, juillet. http://arxiv.org/abs/1807.03675.
Schmidt, Eric. 2005. « Association of National Advertisers ». *Association of National Advertisers* (blog). 8 octobre 2005. http://www.google.com/press/podium/ana.html.
Schmitt, Professor Michael N. 2013. *[(Tallinn Manual on the International Law Applicable to Cyber Warfare)]*. CAMBRIDGE UNIVERSITY PRESS.
Scholte, Jan Aart. 2018. « Internet Governance ». The Routledge Handbook of Transregional Studies. 8 novembre 2018. https://doi.org/10.4324/9780429438233-39.
Seifikar, Mahsa, et Saeed Farzi. 2019. « A comprehensive study of online event tracking algorithms in social networks ». *Journal of information science* 45 (2): 156-68.
Semantic Media wiki. 2013. « Introduction to Semantic MediaWiki ». 2013. http://semantic-mediawiki.org/wiki/Help:Introduction_to_Semantic_MediaWiki.

Semenov, Andrey. 2018. « Protest Event Analysis as a Tool for Political Mobilization Studies ». *Sotsiologicheskoe Obozrenie / Russian Sociological Review* 17 (janvier): 317-41. https://doi.org/10.17323/1728-192X-2018-2-317-341.

Sénat. 2016. « Développement de la prédiction criminelle - Sénat ». 29 décembre 2016. https://www.senat.fr/questions/base/2015/qSEQ150616562.html.

———. 2018. « Commission des affaires étrangères, de la défense et des forces armées : compte rendu de la semaine du 1er octobre 2018 ». 10 mars 2018. http://www.senat.fr/compte-rendu-commissions/20181001/etr.html.

SGDSN. 2019. « Stratégie Nationale du Renseignement – Juillet 2019 | Secrétariat général de la défense et de la sécurité nationale ». juillet 2019. http://www.sgdsn.gouv.fr/evenement/strategie-nationale-du-renseignement-juillet-2019/.

Shapiro, Aaron. 2017. « Reform Predictive Policing ». *Nature News* 541 (7638): 458. https://doi.org/10.1038/541458a.

Sharp, Gene. 2011. *From Dictatorship to Democracy: A Conceptual Framework for Liberation*. London: Green Print.

Shirky, Clay. 2011. « The political power of social media: Technology, the public sphere, and political change ». *Foreign affairs*, 28–41.

Sifter. 2018. « I Need One Year of Historical Twitter and Do Not Have Much Money. How Can I Reduce the Cost? » Texifter. 10 septembre 2018. http://texifter.zendesk.com/hc/en-us/articles/204157430-I-need-one-year-of-historical-Twitter-and-do-not-have-much-money-How-can-I-reduce-the-cost-.

Silver, Laura. 2018. « Western Europeans Under 30 View News Media Less Positively, Rely More on Digital Platforms Than Older Adults ». *Pew Research Center's Journalism Project* (blog). 30 octobre 2018. https://www.journalism.org/2018/10/30/western-europeans-under-30-view-news-media-less-positively-rely-more-on-digital-platforms-than-older-adults/.

Similiar Web. 2019. « Classement des meilleurs sites internet au monde - SimilarWeb ». 8 janvier 2019. https://www.similarweb.com/fr/top-websites.

Singh, Nand Kumar. s. d. « Internet Filtration and Internet Neutrality ». *International Journal of Computer Trends and Technology*. Consulté le 27 août 2019. http://www.ijcttjournal.org/archives/ijctt-v49p124.

Slate. 2013. « Pourquoi ça rame quand je veux regarder une vidéo YouTube avec Free ». Slate.fr. 15 janvier 2013. http://www.slate.fr/story/67161/google-free-video-interconnexion-rame.

Sloan, Luke, Jeffrey Morgan, William Housley, Matthew Leighton Williams, Adam Michael Edwards, Peter Burnap, et Omer Farooq Rana. 2013. « Knowing the Tweeters: Deriving Sociologically Relevant Demographics from Twitter ». *Sociological Research Online* 18 (août). https://doi.org/Sloan, Luke <http://orca.cf.ac.uk/view/cardiffauthors/A2354765.html>, Morgan, Jeffrey <http://orca.cf.ac.uk/view/cardiffauthors/A451039Y.html>, Housley, William <http://orca.cf.ac.uk/view/cardiffauthors/A0243107.html>, Williams, Matthew Leighton <http://orca.cf.ac.uk/view/cardiffauthors/A0088729.html>, Edwards, Adam Michael <http://orca.cf.ac.uk/view/cardiffauthors/A001202G.html>, Burnap, Peter <http://orca.cf.ac.uk/view/cardiffauthors/A065214B.html> and Rana, Omer Farooq <http://orca.cf.ac.uk/view/cardiffauthors/A034253X.html> 2013. Knowing the Tweeters: Deriving sociologically relevant demographics from Twitter. Sociological Research Online 18 (3) , 7. 10.5153/sro.3001

<http://dx.doi.org/10.5153/sro.3001> file <http://orca.cf.ac.uk/49152/1/SocResOnline%20Knowing%20the%20Tweeters.pdf>.
Snow, D., et R. Benford. 1988. « Ideology, Frame Resonance, and Participant Mobilization ». In *From structure to action: comparing social movement research across cultures*, édité par Bert Klandermans, Hanspeter Kriesi, et Sidney G. Tarrow, International social movement research:197-217. Greenwich, Conn: JAI Press.
Snow, David A., E. Burke Rochford, Steven K. Worden, et Robert D. Benford. 1986. « Frame Alignment Processes, Micromobilization, and Movement Participation ». *American Sociological Review* 51 (4): 464-81. https://doi.org/10.2307/2095581.
Sohaib, Athar. 2011a. « Twitter / ReallyVirtual : A huge window shaking bang ... » mai 2011. https://twitter.com/ReallyVirtual/statuses/64783440226168832.
———. 2011b. « Helicopter hovering above Abbottabad at 1AM (is a rare event). » Microblog. *@reallyvirtual* (blog). 5 janvier 2011. https://twitter.com/reallyvirtual/status/64780730286358528.
———. 2011c. « Twitter / ReallyVirtual : Helicopter hovering above ... » 5 janvier 2011. https://twitter.com/ReallyVirtual/statuses/64780730286358528.
Soussi, Seima. 2011. « Comment faire la révolution à l'heure d'internet? » *ARCHIVIO ANTROPOLOGICO MEDITERRANEO on line anno XII/XIII (2011), n. 13 (2)*, 33.
Sputnik News. 2019. « Défense russe: Paris et Bruxelles prépareraient une provocation à l'arme chimique en Syrie ». 29 mars 2019. https://fr.sputniknews.com/international/201903291040547317-france-belgique-preparation-provocation-syrie-armes-chimiques/.
Starbird, Kate, Leysia Palen, Amanda L. Hughes, et Sarah Vieweg. 2010. « Chatter on the Red: What Hazards Threat Reveals About the Social Life of Microblogged Information ». In *Proceedings of the 2010 ACM Conference on Computer Supported Cooperative Work*, 241–250. CSCW '10. New York, NY, USA: ACM. https://doi.org/10.1145/1718918.1718965.
Statista. 2014a. « Active social media penetration in European countries 2014 | Statistic ». Statista. 2014a. http://www.statista.com/statistics/295660/active-social-media-penetration-in-european-countries/.
———. 2019b. « Global Social Media Ranking 2019 ». Statista. 2019b. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.
———. 2019a. « Number of Social Media Users Worldwide 2010-2021 ». Statista. 2019a. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.
———. 2019. « Social Media & User-Generated Content ». Statista. 2 mai 2019. https://www.statista.com/markets/424/topic/540/social-media-user-generated-content/.
Sterling, Bruce. 1993. « A Short History of the Internet ». Hello World! 1993. http://omundy.wordpress.com/2010/01/17/web_1-a-short-history-of-the-internet-by-bruce-sterling-2/.
Stern, Jessica, et J. M. Berger. 2015. *ISIS: The State of Terror*. First Edition edition. New York, N.Y: Ecco.
Stoddard, Jeremy D. 2014. « The need for media education in democractic education ». In .
Stricker, Sarah. 2010. « Online-Spionage: Die schöne Facebook-Freundin der Elitesoldaten ». *Spiegel Online*, 17 mai 2010. http://www.spiegel.de/politik/ausland/online-spionage-die-schoene-facebook-freundin-der-elitesoldaten-a-694582.html.
Stroud, Matt. 2014. « The Minority Report: Chicago's New Police Computer Predicts Crimes, but Is It Racist? » The Verge. 19 février 2014.

https://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist.
Subrahmanian, V. S., Amos Azaria, Skylar Durst, Vadim Kagan, Aram Galstyan, Kristina Lerman, Linhong Zhu, et al. 2016. « The DARPA Twitter Bot Challenge ». *Computer* 49 (6): 38-46. https://doi.org/10.1109/MC.2016.183.
Suremain, Philippe de. 2014. « L'Ukraine en crise, l'Europe fracturée ». *Commentaire* Numéro 148 (4): 741-46.
Syria Deeply. 2013. « Syria Deeply - Syria News ». Syria Deeply - Syria News. 11 mars 2013. http://beta.syriadeeply.org/.
Tarrow, Sidney. 1989. *Democracy and Disorder: Protest and Politics in Italy, 1965-1975*. Oxford : New York: Oxford University Press.
Tarrow, Sidney G. 2011. *Power in Movement: Social Movements and Contentious Politics*. 3 edition. Cambridge ; New York: Cambridge University Press.
The Independent. 2014. « Ukraine Crisis: A Timeline of the Conflict from the Euromaidan ». The Independent. 2 septembre 2014. http://www.independent.co.uk/news/world/europe/ukraine-crisis-a-timeline-of-the-conflict-from-the-euromaidan-protests-to-mh17-and-civil-war-in-the-9706999.html.
Thiele, Ralph. 05/15. « Crisis in Ukraine – The Emergence of Hybrid Warfare ». 347. Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung. https://www.files.ethz.ch/isn/190792/347_Thiele_RINSA.pdf.
Thomas, Sue, Chris Joseph, Jess Laccetti, Bruce Mason, Simon Mills, Simon Perril, et Kate Pullinger. 2007. « Transliteracy: Crossing Divides ». *First Monday* 12 (12). https://doi.org/10.5210/fm.v12i12.2060.
Thonnard, Olivier. 2010. « A multi-criteria clustering approach to support attack attribution in cyberspace ». Theses, Télécom ParisTech. https://pastel.archives-ouvertes.fr/pastel-00006003.
Tilly, Charles. 1978. *From Mobilization to Revolution*. Reading, Mass: Longman Higher Education.
———. 1984. « Les origines du répertoire d'action collective contemporaine en France et en Grande-Bretagne ». *Vingtième Siècle. Revue d'histoire* 4 (1): 89-108. https://doi.org/10.3406/xxs.1984.1719.
Tilly, Charles, et Sidney Tarrow. 2015. *Contentious Politics*. 2e éd. New York, NY: OUP USA.
Tilly, Charles, et Lesley J. Wood. 2012. *Social Movements 1768-2012*. 3e éd. Boulder, CO: Routledge.
Tkacheva, Olesya, Lowell H. Schwartz, Martin C. Libicki, Julie E. Taylor, Jeffrey Martini, et Caroline Baxter. 2013. « Internet Freedom and Political Space ». Product Page. 2013. https://www.rand.org/pubs/research_reports/RR295.html.
Tramp, Sebastian, Philipp Frischmuth, Timofey Ermilov, et Sören Auer. 2010. « Weaving a Social Data Web with Semantic Pingback ». In *Knowledge Engineering and Management by the Masses*, édité par Philipp Cimiano et H. Sofia Pinto, 135-49. Lecture Notes in Computer Science 6317. Springer Berlin Heidelberg. http://link.springer.com/chapter/10.1007/978-3-642-16438-5_10.
Treverton, Gregory F, et Wilhelm Agrell. 2009. *National Intelligence Systems: Current Research and Future Prospects*. New York: Cambridge University Press.
Tucek, Aaron. s. d. « Constraining Big Brother: The Legal Deficiencies Surrounding Chicago's Use of the Strategic Subject List ». *THE UNIVERSITY OF CHICAGO LEGAL FORUM*, 35.
Turse, Nick. 2012. *The Changing Face of Empire: Special Ops, Drones, Spies, Proxy Fighters, Secret Bases, and Cyberwarfare*. Chicago, IL: Haymarket Books.

Tusa, Felix. 2013. « How Social Media Can Shape a Protest Movement: The Cases of Egypt in 2011 and Iran in 2009 ». Arab Media & Society. 2013. https://www.arabmediasociety.com/how-social-media-can-shape-a-protest-movement-the-cases-of-egypt-in-2011-and-iran-in-2009/.
Twitter. 2009. « Down Time Rescheduled ». 15 juin 2009. https://blog.twitter.com/en_us/a/2009/down-time-rescheduled.html.
———. 2019. « Twitter Premium APIs – Twitter Developers ». 2019. https://developer.twitter.com/en/premium-apis.html.
@TwitterSupport. 2019. « (20) Twitter Support sur Twitter : "Most people don't tag their precise location in Tweets, so we're removing this ability to simplify your Tweeting experience. You'll still be able to tag your precise location in Tweets through our updated camera. It's helpful when sharing on-the-ground moments." / Twitter ». Twitter. 18 juin 2019. https://twitter.com/twittersupport/status/1141039841993355264.
UN telecom agency. 2018. « Internet Milestone Reached, as More than 50 per Cent Go Online: UN Telecoms Agency ». UN News. 7 décembre 2018. https://news.un.org/en/story/2018/12/1027991.
Unesco. 2005. « La proclamation d'Alexandrie sur la maîtrise de l'information et l'apprentissage tout au long de la vie ». https://webarchive.loc.gov/all/20131205075344/http://archive.ifla.org/III/wsis/BeaconInfSoc-fr.html.
———. 2013a. « Media and information literacy: policy and strategy guidelines | United Nations Educational, Scientific and Cultural Organization ». http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/media-and-information-literacy-policy-and-strategy-guidelines/.
———. 2013b. « Gouvernance de l'Internet ». UNESCO. 7 mai 2013. https://fr.unesco.org/themes/gouvernance-linternet.
———. 2017. « Fake news : ce qu'en pensent les journalistes ». UNESCO. 18 juillet 2017. https://fr.unesco.org/courier/july-september-2017/fake-news-ce-quen-pensent-journalistes.
U.S. Department of Justice. 2009. « Navigating Your Agency's Path to Intelligence-Led Policing », avril, 30.
U.S. State Department. 2011. « U.S. State Department Social Media Landscape : France ». http://publicintelligence.net/ufouo-u-s-state-department-social-media-landscape-france/.
Valeyre, Bertrand. 2012. *Winning hearts and minds*. Cahier de la recherche doctrinale. https://www.cdec.terre.defense.gouv.fr/contents-in-english/our-publications/old-publications/cahier-de-la-recherche-doctrinale/winning-hearts-and-minds.
VALLS Manuel. 2016. « Déclaration de M. Manuel Valls, Premier ministre, sur le continuum entre la sécurité intérieure et extérieure dans la lutte contre le terrorisme djihadiste, l'opération Sentinelle et le projet de Garde nationale, la nécessité d'une augmentation des efforts de défense de l'Union européenne et le rôle de l'OTAN, à Paris le 6 septembre 2016. » Text. http://www.universite-defense.org, le 19 septembre 2016. 6 septembre 2016. http://discours.vie-publique.fr/notices/163002563.html.
Vander Wal, Thomas. 2007. « Folksonomy ». vanderwal.net. 2 février 2007. http://vanderwal.net/folksonomy.html.
Varol, Onur, Emilio Ferrara, Clayton A. Davis, Filippo Menczer, et Alessandro Flammini. 2017. « Online Human-Bot Interactions: Detection, Estimation, and Characterization ». *arXiv:1703.03107 [cs]*, mars. http://arxiv.org/abs/1703.03107.

Ventre, Daniel. 2010. *Cyberguerre et guerre de l'information: stratégies, règles, enjeux*. Lavoisier.
———. 2011. *Cyberattaque et cyberdéfense*. Paris, France: Hermès science publications : Lavoisier, impr. 2011.
Vieweg, Sarah, Amanda L Hughes, Kate Starbird, et Leysia Palen. 2010. « Microblogging During Two Natural Hazards Events: What Twitter May Contribute to Situational Awareness ». In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 10.
Villani, Cédric. 2018. « Donner un sens à l'intelligence artificielle pour une stratégie nationale européenne ».
W3. 2004. « RDF Semantics ». 4 octobre 2004. http://www.w3.org/TR/2004/REC-rdf-mt-20040210/.
———. 2012. « SKOS Simple Knowledge Organization System ». 13 décembre 2012. http://www.w3.org/2004/02/skos/.
We are social. 2014. « Social, Digital & Mobile in Europe in 2014 ». We Are Social. 5 février 2014. https://wearesocial.com/blog/2014/02/social-digital-mobile-europe-2014.
Weller, Katrin. 2013. *Twitter and Society*. Peter Lang.
White, Micah. 2016. *The End of Protest: A New Playbook for Revolution*. Toronto: Knopf Canada.
Whiting, Anita, et David Williams. 2013. « Why People Use Social Media: A Uses and Gratifications Approach ». *Qualitative Market Research: An International Journal*, août. https://doi.org/10.1108/QMR-06-2013-0041.
Wilkinson, Paul. 1971. *Social Movement*. London: Macmillan.
Won, Donghyeon, Zachary C. Steinert-Threlkeld, et Jungseock Joo. 2017. « Protest Activity Detection and Perceived Violence Estimation from Social Media Images ». In *Proceedings of the 25th ACM International Conference on Multimedia*, 786–794. MM '17. New York, NY, USA: ACM. https://doi.org/10.1145/3123266.3123282.
World bank. 2019. « Urban population (% of total population) | Data ». 2019. https://data.worldbank.org/indicator/sp.urb.totl.in.zs.
World Elections. 2010. « Ukraine 2010 – Runoff ». *World Elections* (blog). 9 février 2010. https://welections.wordpress.com/2010/02/09/ukraine-2010-runoff/.
———. 2012. « Ukraine 2012 ». *World Elections* (blog). 4 novembre 2012. https://welections.wordpress.com/2012/11/04/ukraine-2012/.
Wüest, Bruno, Klaus Rothenhäusler, et Swen Hutter. 2013. « Using Computational Linguistics to Enhance Protest Event Analysis ». In *Wüest, Bruno; Rothenhäusler, Klaus; Hutter, Swen (2013). Using Computational Linguistics to Enhance Protest Event Analysis. In: ENCoRe Workshop « Tools and Techniques for Conflict Event Data Collection », Konstanz, 6 December 2013 - 7 December 2013.* Konstanz: University of Zurich. https://doi.org/info:doi/10.5167/uzh-150416.
Yandex. 2014. « Огляд соціальних мереж і Твіттера в Україні ». https://download.yandex.ru/company/Yandex_on_UkrainianSMM_Summer_2014.pdf.
« Yandex Report: Twitter Usage in Ukraine ». 2014. *Digital East Factor* (blog). b 2014. http://www.digitaleastfactor.com/yandex-report-twitter-usage-ukraine/.
Yardi, Sarita, et Danah Boyd. 2010. « Tweeting from the Town Square: Measuring Geographic Local Networks ». In *Fourth International AAAI Conference on Weblogs and Social Media*. http://www.aaai.org/ocs/index.php/ICWSM/ICWSM10/paper/view/1490.
Yildirim, Pinar, Esther Gal-Or, et Tansev Geylani. 2013. « User-Generated Content and Bias in News Media ». *Management Science* 59 (12): 2655-66. https://doi.org/10.1287/mnsc.2013.1746.
Yu, Manzhu, Chaowei Yang, et Yun Li. 2018. « Big Data in Natural Disaster Management: A Review ». *Geosciences* 8 (5): 165. https://doi.org/10.3390/geosciences8050165.

Zech, Steven T., et Michael Gabbay. 2016. « Social Network Analysis in the Study of Terrorism and Insurgency: From Organization to Politics ». *International Studies Review* 18 (2): 214-43. https://doi.org/10.1093/isr/viv011.
Zelikow, Philip D. 2011. *National Commission on Terrorist Attacks*.
Zhang, Han, et Jennifer Pan. 2019. « CASM: A Deep-Learning Approach for Identifying Collective Action Events with Text and Image Data from Social Media ». *Sociological Methodology* 49 (1): 1-57. https://doi.org/10.1177/0081175019860244.
Zhou, Deyu, Liangyu Chen, et Yulan He. 2015. « An Unsupervised Framework of Exploring Events on Twitter: Filtering, Extraction and Categorization », janvier, 7.
Zolberg, Aristide R. 1972. « Moments of Madness ». *Politics & Society* 2 (2): 183-207.

Table des matières

Table des illustrations