Master Etudes Russes et Post-soviétiques

Année 2023-2024

« Les apports de l'OSINT dans l'étude des conflits armés : le cas de la guerre russo-ukrainienne »

Mémoire de stage au Bureau de l'Observatoire des Conflits
rattaché au Pôle Etudes et Prospectives

Centre de Doctrine et d'Enseignement du Commandement

Commandement du Combat Futur

Ministère des Armées

Par Marion Bretton – 42002715

Sous la direction de Ioulia Shukan

Et

Jean-Robert Raviot

Table des Matières

Remerciements

Tout d'abord, je tiens à remercier Madame Ioulia Shukan et Monsieur Jean Robert Raviot qui ont accepté de diriger ce mémoire de stage de dernière année de Master. Leurs enseignements ont systématiquement été mobilisés dans les missions qui m'ont été confiées.

Je remercie également l'équipe du Bureau de l'Observatoire des Conflits, dont l'expérience a contribué à ma spécialisation dans le domaine de la défense.

Déclaration de travail personnel

Je déclare que **ce rapport ne constitue pas une prise de position officielle de l'Armée de Terre**, restitue des observations personnelles et ne peut être suspecté de plagiat.

Les emprunts cités sont sourcés et référencés dans la bibliographie.

Certaines informations ne pourront pas être restituées, car elles sont issues de documents à diffusion restreinte.

Ce rapport contient des éléments communs à mon rapport d'alternance du Master Risques, Sécurité, Conflits effectué en simultané, également à l'Université Paris-Nanterre et qui sera soutenu en septembre 2024.

Acronymes

CDEC : Centre de Doctrine et d'Enseignement du Commandement

CCF : Commandement du Combat Futur

PEP : Pôle Etudes et Prospectives

BOC : Bureau Observatoire des Conflits

CEMAT : Chef d'Etat-Major de l'Armée de Terre

LCL : grade de Lieutenant-Colonel

OSINT : Open-Source Intelligence

OSINT-V: OSINT verifiée/ Validated OSINT

OSINF : Open-Source Information

ISR : Intelligent Surveillance and Reconnaissance

OSD : Open-Source Data

WWW : World Wide Web

FAFR : Forces Armées de la Fédération de Russie

FAU : Forces Armées Ukrainiennes

SMP : Sociétés Militaires Privées

Introduction

Présentation de la structure

« Si Vis Pacem, Para Bellum »[1], telle est la devise du CDEC que j'ai intégré en juin 2023 en tant qu'analyste russophone des conflits armés, en répondant à une annonce publiée sur le site PASS du Ministère de la Transformation et de la Fonction publique. À la suite de ce premier Contrat Armée Jeunesse (CAJ)[2] de trois mois effectué en M1 ERPS, mon contrat a été transformé en apprentissage d'un an, de septembre 2023 à septembre 2024. Mes observations relèvent donc d'un travail de plus d'un an et traduisent les évolutions du conflit auxquelles j'ai pu être confrontée en tant qu'analyste. Le CDEC, situé sur le site de l'Ecole Militaire, est une structure spécifique au Ministère des Armées, souvent comparée à un « *Think-Tank* », ayant pour rôle de conseiller les hauts responsables de l'Armée de Terre.

Le Bureau de l'Observatoire des Conflits (BOC) pour lequel je travaille encore à l'heure actuelle est dirigé par le LCL Olivier Entraygues, appuyé par une équipe de militaires d'active et de réserve, allant des grades de Commandant à Colonel, ainsi que d'une équipe d'analystes et de cartographes. Chaque analyste travaille sur une zone géographique et doit obligatoirement maîtriser une langue spécifique (russe, arabe, chinois ou turc), ainsi que les méthodes de recherches en sources ouvertes (OSINT).

Le BOC produit mensuellement une brève des conflits ayant pour objectif d'éclairer l'Armée de Terre sur un conflit en cours, non pas sur des thématiques géopolitiques mais uniquement militaires, tactiques et stratégiques. Les principales observations portent sur la géographie des champs de bataille, les équipements utilisés, les effectifs militaires déployés ainsi que la hiérarchie militaire. Il est alors impératif de maîtriser des concepts théoriques militaires et de connaître les éléments doctrinaux auxquels nous devons nous référer pour transposer et adapter les réalités des combats aux connaissances de l'Armée française, dans la mesure du possible.

[1] « Si tu veux la paix, prépare la guerre »
[2] CAJ : un contrat de 3 mois non renouvelable rémunéré au SMIC, idéal pour une première expérience défense

Outre la brève des conflits, chaque équipe constituée d'un ou plusieurs militaires aidés d'un analyste produit des notes de recherches sur des aspects précis des conflits. Ces notes peuvent porter sur des conflits en cours ou potentiels. Les productions écrites sont présentées lors de conférences ou d'interventions organisées uniquement au sein de l'Armée de Terre.

Enfin, ne disposant d'aucune expérience préalable dans la défense ni dans un milieu militaire, aucune formation ne m'a été proposée, j'ai acquis les compétences nécessaires au fur et à mesure, notamment en apprenant du vocabulaire en français et en russe, spécifique au domaine militaire (les grades, les équipements, les acronymes etc.). De même, j'ai dû apprendre ce même vocabulaire en ukrainien pour faciliter mes recherches.

Présentation des missions

A titre personnel, mes missions s'effectuent principalement en sources ouvertes et portent sur le conflit russo-ukrainien. Malheureusement, à défaut d'avoir du matériel professionnel à disposition, ces recherches se font de manière « artisanale » et sur des supports personnels. Les ressources les plus exploitées se trouvent sur *Telegram* ou *VK,* où malgré de nombreuses précautions prises pour rester anonyme, mes données personnelles tel que mon numéro de téléphone sont exposées et potentiellement recueillies. *Telegram* ma' permis d'accéder à des canaux dédiés au conflit russo-ukrainien exposant des données techniques parfois pro-russes, pro-ukrainiennes, relativement objectives, etc. Certains canaux traitent de données socio-militaires, concernant notamment la mobilisation et les manières de la contourner ou encore les pertes humaines par exemple.

De même, ne disposant pas d'un réseau internet ouvert où l'on peut accéder à des pages internet librement, j'effectue mes recherches sur mes propres appareils, nécessitant alors l'installation de *VPN* gratuits tel que Proton et des précautions pour limiter mon empreinte numérique.

A quelques occasions, j'ai toutefois eu l'opportunité de mener des entretiens en russe avec des personnes d'origine ukrainiennes et russes, afin de confirmer ou encore

d'infirmer certaines informations obtenues en sources ouvertes. Ces entretiens se sont déroulés du fait d'une initiative personnelle et n'ont pas été demandés par ma hiérarchie.

Cette méthodologie de travail m'a permis de prendre conscience du degré d'exposition d'un étudiant cherchant des informations en sources ouvertes, dans le cadre d'un travail de recherche par exemple. Ces recherches ne sont en effet pas sans risque, bien que l'on suppose communément et à tort que les enquêtes numériques sont moins dangereuses que certaines enquêtes de terrain.

Présentation de mon travail de recherche

J'ai ainsi choisi d'orienter ce mémoire de stage sur l'utilisation des sources ouvertes dans le traitement du conflit russo-ukrainien. Je souhaite en effet traiter de la manière dont mon expérience au sein du Ministère des Armées m'a permis de restituer des concepts théoriques étudiés en cours à Nanterre et de les compléter par des recherches en sources ouvertes afin d'alimenter les réflexions de mon service. Ce travail a également pour objectif d'identifier les apports des enquêtes numériques vis-à-vis des enquêtes de terrain et la façon dont elles peuvent modifier les perceptions d'une réalité. Enfin, l'OSINT permet de traiter le conflit comme sortant du cadre militaire strict, impliquant des acteurs civils n'appartenant pas aux institutions militaires.

Lors de mon mémoire de recherche de première année de Master ERPS, je m'étais intéressée au phénomène des « influenceurs du religieux » et sur la forme que prenaient leurs engagements dans un terrain numérique. En l'occurrence, ce nouveau travail relevant de l'anthropologie numérique vise davantage à étudier ces mêmes engagements numériques individuels et collectifs dans un contexte de guerre. La complexité de cet objet d'étude est la constante évolution des pratiques et l'obsolescence rapide des observations. Outre ces difficultés, il faut faire face à de nombreuses contradictions dans la manière de considérer l'outil numérique : comme l'anthropologue Daniel Miller le relève, les contradictions de l'anthropologie digitale

résident principalement dans la dualité entre liberté d'expression et outil de contrôle : « Ethnography will show how digital technologies produce both new possibilities for political activism and also for state oppression »[3].

Les études de Miller contribuent à une meilleure compréhension des subtilités de l'enquête numérique dans un cadre sociologique, ce qui constitue une première base dans mon travail de recherche. Néanmoins, le contexte du conflit armé n'est pas un paramètre pris en compte dans cette étude, il devient alors nécessaire d'adapter les théories de Miller et de les confronter aux comportements des acteurs en temps de guerre.

Les premières questions qui me viennent alors à l'esprit sont les suivantes : l'anthropologie digitale s'adapte habituellement aux subtilités culturelles de la communauté numérique, mais ces subtilités existent-t-elles toujours en temps de guerre ? Le public ciblés par les différents canaux de diffusion change, les acteurs prennent-t-ils alors en compte ces spécificités pour porter leur cause et leur activisme politique ? Autrement dit, ces acteurs ajustent-t-ils leur contenu en fonction du public international et local ?

Les interrogations suivantes portent sur le public auquel on s'intéresse lorsque l'on mène des enquêtes numériques : Miller relève que l'anthropologie numérique étudie principalement les populations vulnérables, moins aisées, en difficultés. Cela s'applique particulièrement à mon travail de recherche, puisque les messageries cryptées *Telegram* et *Whatsapp* offrent la possibilité de s'exprimer à des acteurs « ordinaires », ne disposant pas de fonctions particulières. Ces acteurs sont en effet les plus affectés par un conflit. Le phénomène des « communautés numériques » *(Online communities*) répond ici sans doute à un manque de prise en compte de ces acteurs par les gouvernements et les structures étatiques dans le « réel ».

La difficulté qui émerge face à cette modalité de recherche, contrairement à l'enquête sociologique traditionnelle de terrain, est le risque de la déshumanisation de l'écran : les faits ne sont pas systématiquement traités de manière réelle. Consulter une vidéo dans laquelle apparaissent les corps de soldats tombés sur le champ de bataille ne produit pas le même effet que de se trouver face à ces corps dans la vie réelle. La réalité tangible fait ici défaut. Comme le rappelle justement Miller : "Nobody lives

[3] MILLER, Daniel, (2018) 2023. "Digital anthropology". In The Open Encyclopedia of Anthropology, edited by Felix Stein. Facsimile of the first edition in The Cambridge Encyclopedia of Anthropology

just online, so to understand their involvement with digital technologies we continue to focus on the wider context of their non-digital lives".[4] Il est en effet important de considérer l'outil numérique comme une continuité de la vie réelle ou « non-numérique » et non comme une réalité alternative.

[4] MILLER, Daniel, (2018) 2023. "Digital anthropology". In The Open Encyclopedia of Anthropology, edited by Felix Stein. Facsimile of the first edition in The Cambridge Encyclopedia of Anthropology

Partie I – Les données ciblées en source ouverte dans l'étude du conflit russo-ukrainien

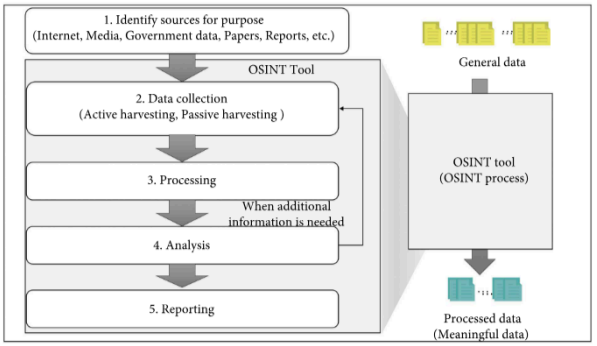
Lorsque des recherches sont effectuées dans le cyber espace à des fins d'évaluation tactique et stratégique d'un conflit, des données de natures diverses et variées affluent et doivent être traitées avec méthodologie. Afin de comprendre la nature d'une décision politique militaire, il est nécessaire d'examiner le narratif des belligérants et sa diffusion. Au contraire, si l'on cherche à évaluer un dysfonctionnement sur le champ de bataille, les discours individuels des usagers sont révélateurs. Les données objectives concernant le matériel et l'imagerie, plus largement, sont dorénavant accessibles sur des canaux de diffusions professionnalisés dans le traitement des combats sur le champ de bataille. Enfin, les données chiffrées telles que des coordonnées GPS ou encore le nombre de pertes humaines et matérielles sont les plus complexes à traiter uniquement en OSINT et en OSINF.

Afin d'illustrer la méthodologie utilisée afin de collecter des informations en OSINT, plusieurs schémas ont été élaborés depuis 2022 :[5]

Les données rendues ouvertes et accessibles sont perçues comme un signe de transparence de la part d'un État vis-à-vis de sa population et donc, en temps de guerre, il s'agit d'un outil de communication essentiel. Dès les années 2015, Anna Ignatova[6] détaillait dans un article l'importance pour un état de publier ouvertement des données concernant des prises de décisions et des informations sur le secteur public. Cela permet d'impliquer les populations et de donner l'illusion d'une transparence absolue. Toutefois, pour que cette

Figure 1

Structure of OSINT.



[5] HWANG Yong-Woon, LEE Yeong, KIM Hwankuk, LEE Hyejung, and KIM Donghyun, Current Status and Security Trend of OSINT, Hindawi, 18/02/2022

[6] ИГНАТОВА Анна Михайловна, ОТКРЫТЫЕ ДАННЫЕ КАК НОВЫЙ СПОСОБ ВЗАИМОДЕЙСТВИЯ ГОСУДАРСТВА И ОБЩЕСТВА, ГРАМОТА, 2015

transparence soit réelle, il est nécessaire que l'Etat soit qualifié de démocratique[7]. En effet, autoriser l'accès à des données publiques à sa population peut également être un moyen détourné de diffuser de la désinformation. Or, le gouvernement russe est particulièrement réputé pour maîtriser cette stratégie. En accélérant le flux d'informations jugées fiables car diffusées par l'État, les populations sont soumises à de la désinformation et deviennent sensibles à la propagande. Néanmoins, l'un des effets inverses de cette stratégie est de pousser les populations à éviter les chaînes et les canaux officiels diffusant des informations issues de l'Etat, afin d'éviter d'être influencées par la propagande. Dans ce contexte de guerre où la désinformation est soupçonnée d'être partout, certains choisissent de faire leurs propres recherches afin de déceler la vérité. Une fois encore l'OSINF et l'OSINT offrent aux populations des moyens alternatifs afin d'obtenir des informations.

Les chiffres

Les données les plus communément recherchées en OSINT dans le cadre de l'étude d'un conflit armé sont les chiffres. En effet, les belligérants ne communiquent que très peu sur leurs chiffres, surtout s'ils sont à leur désavantage. Concernant le matériel, les chiffres dévoilés par les différents gouvernements servent à accentuer les pertes ennemies ou au contraire, à minimiser les leurs. Il en va de même pour le personnel et non pas seulement le matériel. Par exemple, un gouvernement à davantage intérêt à gonfler les chiffres des pertes civiles afin de montrer la cruauté de son adversaire, tout en minimisant ses pertes militaires, afin de ne pas mettre en cause la qualité de son armée. Ainsi, le gouvernement ukrainien communique régulièrement sur ses pertes civiles, et très peu sur les pertes humaines militaires. De la même manière, le gouvernement russe diffuse un taux de pertes élevé chez les FAU et minime chez les FAFR. Lorsqu'il est question de la transparence de l'État, les chiffres relatifs aux pertes humaines en temps de guerre ne peuvent pourtant pas être dévoilés, sous peine de nuire à la conduite des opérations. Cela risquerait d'entraver grandement la mobilisation, et de jouer sur le moral des troupes engagées.

[7] Дарменова Аида Советовна, Мамыкова Жанл Джумангалиевна, Андерсен Ким Норманн, ОТКРЫТЫЕ ДАННЫЕ: ДВАДЦАТИПЯТИЛЕТНЯЯ ИСТОРИЯ РАЗВИТИЯ, Экономика и бизнес, 2020

De fait, le gouvernement ukrainien a choisi de qualifier ces données de secret d'Etat. Certains analystes indépendants ont choisi d'effectuer des comptages à partir de données en sources ouvertes. En guise d'exemple, on peut citer le blog russe LostArmour[8] qui détaille le nombre de pertes humaines des FAU en s'appuyant sur des rubriques nécrologiques de communes diffusées sur les sites de la commune, ainsi que sur les journaux ukrainiens détaillants la remise de médailles à titre posthume. Ces chiffres, probablement inexacts car incomplets, servent d'indicateurs pour d'autres paramètres, tels que la moyenne d'âge des combattants ou encore leur origine (ukrainien ou engagé international). Ce site est ici est ici sujet à caution, car son propriétaire est ouvertement pro-russe : pourtant, les chiffres relatifs aux pertes s'éloignent grandement des chiffres données par le Kremlin. Par la suite, le scandale des *Pentagon Leaks*[9] d'avril 2023 révéla des chiffres proches de ceux dévoilés par LostArmour. Une fois encore, l'un des problèmes survenu à la suite de cette fuite a été la diffusion de capture d'écran modifiée indiquant des chiffres davantage favorable à Moscou, relayés en masse sur les canaux *Telegram* russes. Nous reviendrons sur la fiabilité des sources dans une seconde partie.

Les données d'intérêt militaire : l'imagerie et la cartographie du champ de bataille

Afin d'élaborer des cartes référençant les actions des FAU et des FAFR sur le théâtre des opérations militaires, la veille en OSINT est un outil inestimable. En effet, le quotidien des combattants est quasi systématiquement documenté et filmé puis retranscrit sur des canaux de diffusion en ligne. Cela permet aux belligérants notamment de témoigner, directement (par des canaux officiels) ou indirectement (par des canaux privés) de leurs progrès et de leurs avancées. Le public ciblé par ces canaux est essentiellement militaire ou du moins, lié au domaine militaire, mais le rapport entre les administrateurs des canaux et le public est unilatéral. Le but est de diffuser une information afin qu'elle soit absorbée par le public, sans solliciter une interaction en retour.

[8]Site de LostArmour https://lostarmour.info/

[9] BBC News, What the leaked Pentagon documents reveal - 8 key takeaways, 15 April 2023, By Paul Adams, Jean Mackenzie and Antoinette Radford

Les outils les plus ciblés par les analystes sont les *Live Maps*, fournis par différents partis (russes, ukrainiens, occidentaux etc.). Les exemples les plus consultés offrant des données géospatiales à l'heure actuelle sont les sites de *DeepStateUA*[10](ukrainien), *Petrenko*[11] (russe) ou encore *Scribble Map*[12] (basé au Canada). Certains d'entre eux, dont *Petrenko,* sont des *reporters* de guerre volontaires, souvent affiliés à leur gouvernement. Ce qui est intéressant d'étudier, au-delà de l'apport technique, est la « professionnalisation » des acteurs ordinaires dans la conduite des opérations. Dotés de certaines compétences techniques comme le traitement de données géospatiales, certains acteurs participent indirectement au conflit en alimentant des canaux rapportant quotidiennement les actions de leurs armées. Les leviers et les motivations reposent souvent sur le patriotisme, ou encore sur la volonté de contribuer à la guerre sans s'y exposer physiquement. L'utilisation de leurs compétences techniques risque effectivement de ne pas être exploitées s'ils s'enrôlent en tant que soldats du rang. Pour autant, en témoignant activement de leur soutien aux opérations, ils contribuent à l'effort de guerre. Outre la forme individuelle que peut prendre cette participation technique dans le conflit, il existe des groupes d'individus, civils et militaires, réunis autour des mêmes idéologies qui « s'autoproclament » reporters, ou qui acquiert ce statut du fait de la notoriété croissante dont ils bénéficient au fil de la documentation des opérations. Il reste néanmoins difficile d'accéder à l'identité précise ou au statut professionnel d'avant-guerre des administrateurs de ces canaux *Telegram* : certains journalistes professionnels se cachent derrière ces profils.

Le cas du groupe *Arkhangel spetsnaza*[13] illustre le cas de mobilisations de militaires (parachutistes, en l'occurrence) qui choisissent de documenter leur quotidien sur le front en diffusant des données géospatiales ou encore de l'imagerie. Les informations sont diffusées sans se positionner comme narratif officiel de l'État, tout en servant les intérêts et la propagande de l'État. On peut envisager que l'objectif est de décentraliser l'information en ne passant pas par des canaux officiels, ce qui a pour effet de rendre les actions plus « réelles », « authentiques » voire « légitimes » car elles n'apparaissent pas contrôlées par un gouvernement de prime abord. Il reste

[10] https://deepstatemap.live/en#6/49.438/32.053
[11] https://t.me/s/petrenko_IHS
[12] https://widgets.scribblemaps.com/sm/?d&z&l&mt&gc&mv&id=091194
[13] https://t.me/s/rusich_army

cependant difficile de discriminer avec précision les objectifs derrière l'existence de ces différents canaux, il ne s'agit donc que de suppositions.

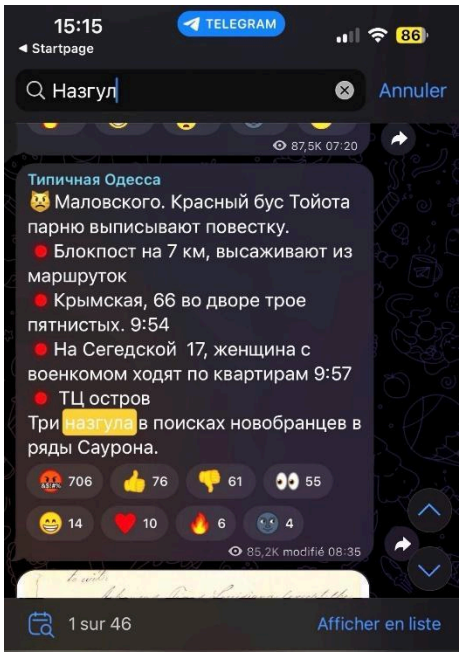
Les phénomènes sociologiques et politiques

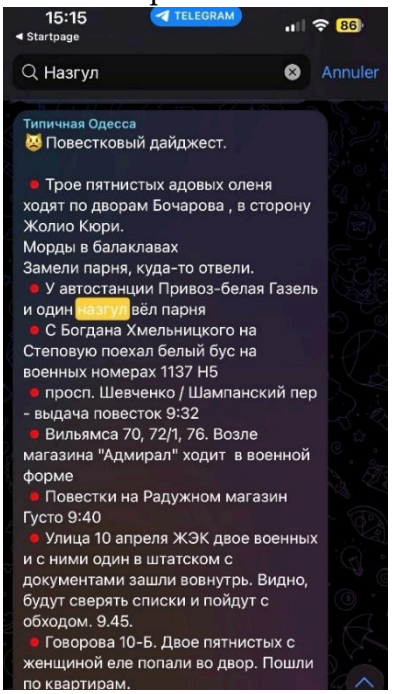
Moins concrets et factuels que les chiffres ou encore l'imagerie, les phénomènes les plus révélateurs étudiés en OSINT sont les tendances dans l'opinion publique ordinaire. En effet, les blogs et les canaux *Telegram* offrent un excellent aperçu des réactions ordinaires en temps de guerre, des formes que peuvent prendre la mobilisation des populations et de l'état de l'opinion publique d'un pays en guerre.

Le phénomène des Sociétés Militaires Privées (SMP) est l'un des éléments du conflit russo-ukrainien le plus préoccupant pour les institutions militaires internationales. En effet, la popularité de certains groupes comme Wagner a conduit les observateurs et les analystes à s'intéresser attentivement à leurs faits et gestes, largement retranscrits sur les réseaux sociaux et les messageries cryptées. Ce phénomène a pris de l'ampleur sur le plan sociologique et politique lors de la « Rébellion Wagner » le 23 juin 2023, illustrant les clivages de l'opinion russe face aux succès des SMP jugés supérieurs à ceux des FAFR. Cela a largement traduit la montée en puissance des SMP en Russie et la défiance vis-à-vis du pouvoir. Une partie des populations russes suivant le quotidien des SMP sur les réseaux sociaux étaient prête à les soutenir face au ministre russe de la défense. Or, cela a indirectement permis au pouvoir russe d'appréhender cette popularité et son ampleur et d'y mettre un terme en interrompant les activités des SMP, dont la médiatisation a cessé depuis la rébellion. La volonté de s'éloigner de la presse traditionnelle pour soutenir de manière spécifique et localisée des forces armées, outre les FAFR de manière générale, s'est répandue. Il arrive également que ces tendances aillent directement à l'encontre des décisions politique des gouvernements et que les contestations prennent la forme de « cyber mobilisations ».

Par exemple, les pages *Telegram* « *типичный* » suivi du nom d'une ville (exemple : *типичная Одесса*) servent souvent de canaux de diffusion afin de révéler les positions des agents des centres de recrutements (*ТЦК*) ukrainiens cherchant à délivrer des ordres de mobilisation. Les personnes suivant ces canaux donnent l'alerte afin de contourner la mobilisation. La communauté *Telegram* de ces pages est allée jusqu'à utiliser des noms de codes afin de désigner les agents des centres de recrutement, qu'ils appellent des *Nazgul* (en référence aux cavaliers noirs du *Seigneur des Anneaux, cf les captures d'écran ci-jointes*).

Cela pourrait s'apparenter à une forme d'activisme numérique ayant pour but de contourner voire entraver les actions du gouvernement ukrainien quant à la mobilisation.





Ce phénomène peut être qualifié de net'activisme, au sens employé par des études antérieures, telle que celle de Michel Brunier :

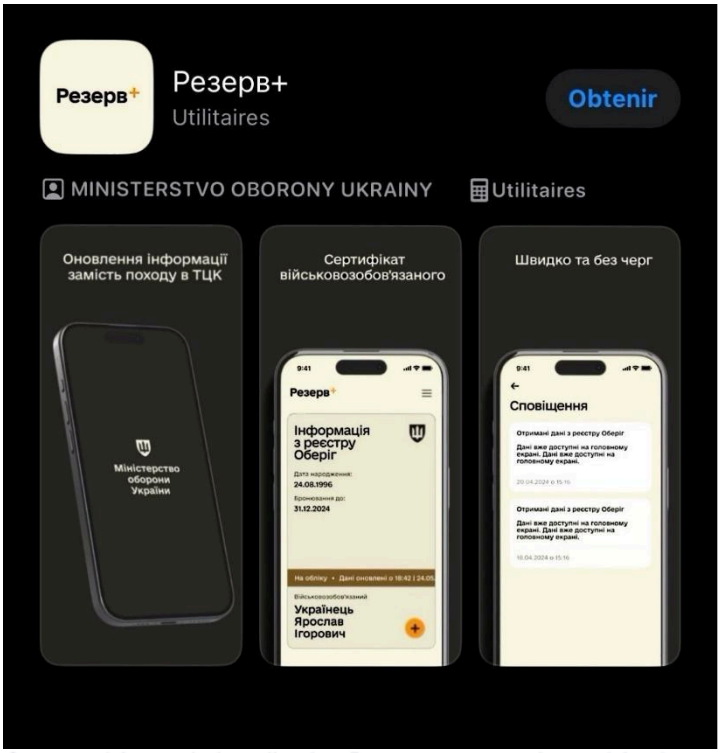
> « Il convient pourtant de bien distinguer ce qui relève ou pas du net'activisme (ou cyberactivisme). Au sens où cela est entendu ici, ne relèvent pas de l'activisme sur la Toile les propagandes unilatérales qui cherchent seulement à convaincre et à obtenir une adhésion. En revanche, appartiennent à ce type d'action les messages cherchant à changer les choses sans passer par des intermédiaires institutionnels et en suscitant la participation directe des acteurs sociaux sollicités, c'est-à-dire en mettant sur un pied d'égalité les émetteurs et les récepteurs d'informations. »[14]

Contrairement aux groupes *Telegram* évoqués précédemment traitant de l'imagerie et des données à caractère militaire, ces canaux sont « participatifs ». Ils font appel à une communauté afin d'obtenir des informations utiles à cette même communauté. Ces observations mènent à repenser le conflit dans sa totalité et à s'intéresser aux nouvelles tendances générées par ce conflit au sein d'une société dans le cyber espace.

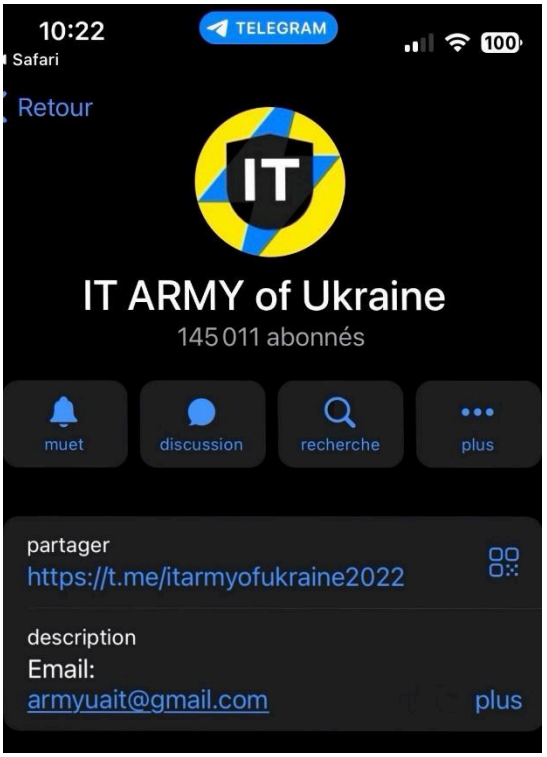
[14] BURNIER Michel, Un nouvel activisme sur l'Internet ?, pages 103 -104, 2009

Partie II – Les particularités et les failles de l'OSINT dans un fait social et anthropologique total[15] telle que la guerre

Le sociologue Marcel Mauss qualifie la guerre de « fait social total », dans le sens où toutes les institutions étatiques sont certes mobilisées, mais toutes les sphères de la société également, et donc tous les acteurs. Le cas du conflit russo-ukrainien illustre parfaitement cet aspect « total » de la guerre, et cela se reflète dans les activités numériques ukrainiennes depuis l'invasion russe de 2022. Par exemple, le gouvernement ukrainien s'est adapté en numérisant une grande partie de ses services à destination de sa population : le recensement des personnes mobilisables se fait sur une application mobile par exemple (l'application *Reserve+*). De plus, une des réponses militaires apportées par l'Ukraine face à la Russie est la création d'une *IT Army of Ukraine*[16]. *L'IT Army*, une nouvelle fois, témoigne de la totalité du phénomène guerrier, puisque des volontaires et des bénévoles de tous les pays alliés de l'Ukraine sont invités à prendre part aux « combats numériques ».



Capture d'écran de l'application Reserve+ proposée sur l'Apple Store



Capture d'écran du canal Telegram officiel de l'IT Army

[15] Expression attribuée à Marcel Mauss, selon un article de Jean-Vincent Holeindre, Ce que la guerre fait aux sociétés, Dans La guerre (2014), pages 5 à 12

[16] Site officiel de l'IT Army https://itarmy.com.ua/

Dans son essai “The Weaponisation of Everything : A Field Guide to the New Way of War”[17], Mark Galeotti évoque la mobilisation de chaque aspect de la société (economic, information and cultural warfare etc.) dans la guerre afin de se détourner d’un conflit ouvert et frontal. Pourtant, la particularité du conflit russo-ukrainien est qu’il combine à la fois la mobilisation de moyens « détournés », « non-traditionnels », pour ne pas dire des moyens « hybrides » de conduire la guerre, tout en revenant à des méthodes guerrières anciennes telle que la guerre des tranchées.

La guerre en Ukraine a contribué à créer de nouvelles tendances dans les comportements numériques des populations et dans leur réponse à la guerre, à plein d’échelle différentes. Si l’enquête numérique est alors un outil précieux afin de conduire des recherches en temps de guerre sans s’exposer physiquement aux combats, il n’en demeure pas moins qu’elle ne serait, au mieux, que complémentaire à une enquête de terrain. Certains aspects du numérique apportent des éléments nouveaux et révélateurs aux enquêtes, en particulier l’anonymat. Néanmoins, les paramètres tels que la fiabilité des sources et les avancées de l’Intelligence Artificielle remettent considérablement en question la crédibilité du travail de recherche. De surcroît, la collecte des données met potentiellement en péril le chercheur ainsi que les internautes.

La vérification des sources et leur objectivité dans un contexte d’émergence de l’Intelligence Artificielle : entre le virtuel et le réel

Lorsque l’on travaille en source ouverte, il convient de distinguer l’OSINT et l’OSINT-V (vérifié) : chaque source est sujette à caution jusqu’à sa vérification par des preuves concrètes comme une observation ou un rapport de source officielle, permettant de traiter la source en toute sécurité. Malgré cela, bien que plus sûre, la source ne peut être considérée comme entièrement fiable. Une fois encore, cela souligne la dualité dans le rapport entre enquête de terrain et enquête numérique. L’enquête numérique peut alors servir de guide à une enquête de terrain afin de

[17] GALEOTTI, Mark, The Weaponisation of Everything: A Field Guide to the New Way of War, Yale, Yale University Press, 2022, 248 p.

l'orienter au préalable. Sans cette enquête de terrain, les vérifications deviennent difficiles.

De plus, la rapidité avec laquelle les technologies de l'intelligence artificielle évoluent est inquiétante pour les enquêtes en OSINT, car les données sont systématiquement remises en question. Les discours des acteurs ordinaires, en revanche, sont moins touchés par cette avancée technologique.

L'exemple le plus célèbre de l'usage de *deep fake* dans le conflit est la vidéo mettant en scène le président ukrainien Volodimir Zelensky annonçant la reddition de l'Ukraine[18]. Cette dernière a eu pour effet la prise de conscience de l'ampleur de l'utilisation des nouvelles technologies dans la manipulation et la désinformation. Tout en étant identifiée instantanément comme « fausse », cette vidéo a pourtant engendré un scepticisme de masse et parfois démesuré des populations envers les contenus auxquels elles pouvaient être exposées. Le « *fact checking* » ou la vérification n'est pas systématiquement possible ni acquise, ce qui entraîne potentiellement une perte totale de confiance des auditeurs envers les informations qui leur sont dévoilées. Le phénomène des « *deep fake* » nuit à la recherche d'imagerie et de fichiers audio/vidéos, tout en influençant *de facto* les opinions du public, voire en les réorientant vers de nouvelles sources d'informations systématiquement. Certains chercheurs en Intelligence Artificielle tels que Hubert Etienne se sont déjà interrogés sur la relation entre les *deepfakes* et le manque de confiance. En effet, le manque de confiance est souvent déjà constaté dans une société avant même l'intervention de la manipulation via l'utilisation de *deepfakes*. Les acteurs, comme par le passé, s'adaptent aux techniques de désinformation et les contournent *in fine* :

> « Still, ceasing to believe in everything does not result in distrusting everyone, and this is why social relativism on truth does not necessarily lead to nihilism on trust. Reducing our passive systematic benevolence towards all information coming from cyberspace should also lead us to search more actively for trustworthy sources and redesign the map of our trust relationships around a network of key people. With the condition of securing authentic identification together with information

[18] EURONEWS, Deepfake Zelenskyy surrender video is the 'first intentionally used' in Ukraine war, 16 mars 2022 consultée le 5/06/2024

> traceability—for instance through blockchain solutions to rapidly identify the original source of a piece of information—we should observe the emergence of a new kind of authority, personified by actors sharing well-verified information on a regular basis".[19]

Etant donné que le rôle d'analyste OSINT des conflits armés repose sur une meilleure compréhension, une appréciation d'une situation, et surtout, une analyse de certaines tendances, l'exactitude parfaite des faits n'est pas recherchée. L'OSINT permet davantage une appréciation subjective des comportements et des réactions à l'échelle humaine dans le conflits, les informations objectives relèveront quant à elles d'autres techniques de recherches et de renseignement.

L'impact de l'anonymat dans le discours numérique

Comme mentionné précédemment, les enquêtes anthropologiques en ligne sont complémentaires des enquêtes de terrain lorsque l'on s'intéresse à des phénomènes humains. Pour autant, lorsque l'on s'exprime sur une messagerie cryptée en ligne, l'anonymat est l'un des facteurs déterminant à prendre en considération et qui diffère de l'enquête de terrain. Bien que l'anonymat demeure une composante préexistence dans les enquêtes sociologiques traditionnelles, son utilisation diffère lorsqu'il s'agit de s'exprimer en ligne.

L'anonymat peut en effet simplifier, voire encourager, des comportements en dehors des normes d'une société puisque le cyber espace semble ôter toute forme de vulnérabilité: "Anonymous online spaces may provide these self-presentational opportunities due to the reduced feelings of vulnerability and judgment from others, along with increased group salience (Grieve & Watkinson, 2016; Spears & Lea, 1994; Turkle, 1995)."[20] Ce constat, bien que généraliste, s'applique également en temps de guerre, particulièrement dans le cas de la guerre russo-ukrainienne qui divise les sociétés. Par exemple, il sera plus facile pour un citoyen russe de s'exprimer sur sa perception du conflit de manière anonyme en ligne que dans l'espace publique russe.

[19] ETIENNE Hubert, The future of online trust (and why Deepfake is advancing it). AI Ethics 1, 553–562 (2021).
[20] Nitschinsk, L., Tobin, S. J., Varley, D., & Vanman, E. J. (2023). Why Do People Sometimes Wear an Anonymous Mask? Motivations for Seeking Anonymity Online. Personality and Social Psychology Bulletin, 0(0).

De fait, on constate une prise de libertés significatives dans les *chats*/ discussions en ligne, particulièrement lorsque l'on ajoute à cela le paramètre de l'éphémère du *chat*. Il est aujourd'hui possible sur toutes les messageries d'activer une option rendant automatique l'autosuppression des interactions. Couplée à l'anonymat, cela renforce le sentiment de liberté d'expression des internautes. Ce phénomène se traduit souvent par des formes de provocations en ligne dans des espaces de discussion, ou encore par l'adhésion ou le soutien à des positions extrêmes. Outre les propos, un imaginaire entier découle de cette liberté d'expression exacerbée avec le recours à des photos de profils ou des pseudonymes permettant la création d'une identité alternative. Afin d'identifier et de comprendre ces mécanismes, l'analyste OSINT doit être sensible aux références et aux subtilités civilisationnelles de la zone ciblée. De manière extrême, certains interlocuteurs se permettent de diffuser des contenus sensibles (vidéos de corps, profanation, violences et insultes) sous couvert de l'anonymat. Leurs auditeurs vont réagir à ce contenu, également de manière anonyme et surtout, démesurée, puisqu'ils ne sont exposés à ces réalités violentes que derrière un écran. Pour des raisons d'éthique personnelle et bien que confrontée à cela durant l'exercice de mes fonctions, je fais le choix de ne pas partager et de simplement mentionner ces contenus dans ce développement.

Cette exposition et cette diffusion de la violence par l'intermédiaire d'interlocuteurs anonymes entraînent plusieurs conséquences à prendre en compte : elle contribue à minimiser voire normaliser des violences allant à l'encontre de toutes normes éthiques et morales d'une société, amplifiées en temps de guerre. Une fois encore, l'anonymat permet de s'affranchir des normes, et cela risque de s'accentuer avec la diversification des plateformes d'échange en ligne et le manque de contrôle sur ces plateformes.

Il ne faut pourtant pas négliger le fait que malgré les précautions, l'anonymat complet reste difficile à obtenir, à partir du moment où les flux de communications et d'échanges dépendent d'infrastructures materielles (de serveurs, de DATA storage centres etc). Ainsi comme le souligne Paolo Palimieri, "Several governments effectively control, monitor, or censor Internet traffic, either during crises or

permanently. Internet protocols have not been designed for privacy and anonymity, and therefore Internet users can also be easily traced and identified."[21]

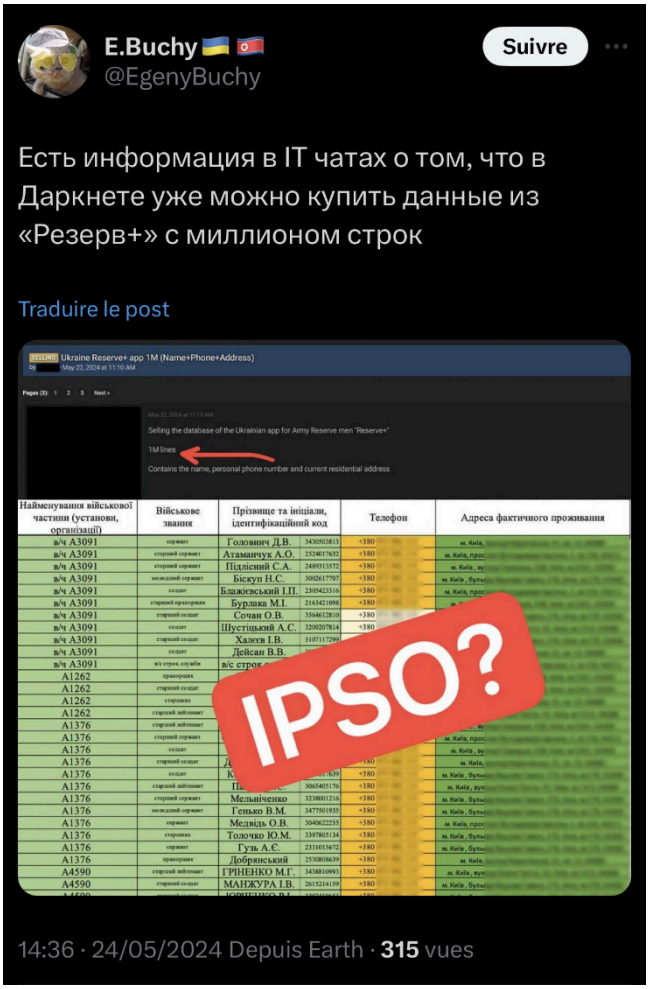
La collecte et le stockages des données numériques, un outil pour les régimes autoritaires ?

"Data is regarded as at least analogous to the traditional role of capital, creating the conditions for more targeted commodification and new forms of power. Datafication gives unprecedented capacities for surveillance and control which not only predict, but also shape and modify human behaviour."[22]

Le stockage des données numériques est encore peu abordé par les sociologues, mais il présente un enjeu clef dans le futur. Les gouvernements font d'ores et déjà majoritairement usage de l'OSINT dans l'ISR, ce qui témoigne de la potentielle dangerosité de cet outil en cas de conflit. Comme évoqué précédemment, l'informatisation des services d'État en lien avec le conflit soulève des enjeux sécuritaires majeurs. En effet, la récente loi de mobilisation ukrainienne prévoit le recours à la digitalisation des données des réservistes ukrainiens afin de faciliter leur identification et leur mise à disposition auprès des Centres de Recrutement Territoriaux. Quelques jours après la sortie de l'application, la mise aux enchères sur le *dark web* des données recensées (plus d'un million de personnes) auraient été observées et diffusées sur les réseaux sociaux, comme le montrent les captures d'écran ci-dessous :

[21] PALMIERI Paolo, Anonymity Networks and Access to Information During Conflicts: Towards a Distributed Network Organisation, 2016 8th International Conference on Cyber Conflict and Cyber Power, 2016, NATO CCD COE Publications, Tallinn

[22] MILLER, Daniel, (2018) 2023. "Digital anthropology". In The Open Encyclopedia of Anthropology, edited by Felix Stein. Facsimile of the first edition in The Cambridge Encyclopedia of Anthropology



Afin d'illustrer la dangerosité du stockage de données à caractère militaire, il est possible de comparer ce stockage à celui de données biométriques dans un conflit armé.

A titre d'exemple, les travaux de Katja Jacobsen Lindskov et de Karl Steinacker[23] alertent sur les risques encourus par les populations ayant été concernées par un recensement biométrique durant la guerre d'Afghanistan afin de bénéficier de l'aide internationale. Une fois Kaboul reprise par le gouvernement taliban, ces centres de stockages de données abandonnés ont permis au Talibans d'identifier les bénéficiaires de l'aide internationale comme « traîtres » et « collaborateurs ». Le risque pourrait être le même à l'issue du conflit russo-ukrainien. Les populations ayant laissé des traces numériques de leurs actions ou de leurs prises de positions s'exposent à des poursuites judiciaires, voire, à des représailles. Différents scénarios

[23] Jacobsen Lindskov Katja, Steinacker Karl, "Contingency Planning in the Digital Age: Biometric Data of Afghans Must Be Reconsidered", PRIO blog, 2021: consulté le 20/11/2023

sont en effet envisageables : les Ukrainiens ayant collaboré avec la Russie et relayé leur soutien au FAFR sur des plateformes en ligne pourraient encourir des sanctions en cas de victoire de l'Ukraine sur la Russie. A l'inverse, les populations s'étant opposées à l'invasion russe encourent un grave danger si le gouvernement russe parvient à prouver leur prise de position en ligne. Les issues possibles sont multiples et les dérives envisagées encore plus inquiétantes, en fonction du degré d'autoritarisme du régime politique ayant accès à ces données. Un simple « j'aime » sur un post pourrait alors avoir des conséquences. En menant eux-mêmes des enquêtes en OSINT, les gouvernements peuvent accéder à des informations compromettantes sur leur propre population. Un gouvernement qui prend le contrôle d'un territoire prend potentiellement le contrôle de ces centres de stockage de données, voire des centres de stockages de données d'un autre gouvernement qui auraient été délocalisés. Dans le cyberespace, il est difficile de faire disparaître des données, des enquêtes plus poussées permettent d'accéder à des contenus effacés. L'espoir repose alors sur le coût et le temps que ces enquêtes prendraient afin d'incriminer une personne, ce qui semble alors peu rentable.

Conclusion

Conclusion quant à l'objet d'étude

L'OSINT peut être davantage révélateur pour une étude sociologique sur les habitudes des populations, plus que dans le domaine du renseignement en lui-même. Les progrès technologiques peuvent déformer une information objective, mais difficilement un discours subjectif, ne pouvant exister ni être conceptualisé autrement que par le cerveau humain. L'analyste en cyber défense Zaki Khalid note à propos du renseignement en source ouverte : "In matters such as Area Studies where knowledge of a country and its geography is concerned, collection officers who do not have knowledge of social sciences will most likely fail to define the scope of effort and what their information sources should be".[24] Il est communément admis dans certaines sociétés et auprès de certains gouvernements qu'un analyste en OSINT doit être qualifié en informatique et en programmation, alors qu'en réalité, sans la connaissance sociologique d'un terrain numérique, les informations récoltées sont inexploitables. En effet, il est absolument nécessaire de combiner une aire d'expertise avec la connaissance de l'OSINT afin d'en tirer le maximum d'information et d'analyse possible. Le manque de connaissance d'un terrain d'étude entraîne des confusions: "Too often, OSINT practitioners look at the sexy topics, when what we need is the mundane"[25].

De même que la guerre, l'évolution numérique a pour effet de transformer des habitudes et de les faire évoluer rapidement : "The possible changes brought about by the Internet/Web in information processing holds the promise of greater innovation in response to the problems of an increasingly complex world; but it can also lead to higher levels of fear, anxiety and alienation that so often accompanies the loss of habits and traditions that add stability to our lives".[26]

L'OSINT dans l'étude d'un conflit armé est un outil de grande valeur, à condition qu'il soit exploité par des analystes ayant suivi des enseignements en sociologie, en

[24] KHALID Zaki, Social Sciences and Interdisciplinarity in OSINT Analysis, Medium, 9/12.2023 consulté le 04/04/2024
[25] LOMAS Dan, The Death of Secret Intelligence? Think Again, Royal United Service Institute, 05/07/2023
[26] GLASSMAN Michael, MIN Ju Kang, Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT), Computers in Human Behavior, Volume 28, Issue 2, March 2012, Pages 673-682

histoire ou encore en anthropologie. L'enquête de terrain traditionnelle reste indispensable à la compréhension d'un phénomène ou d'une tendance.

Appréciations portant sur le stage et le Master ERPS

Cette longue expérience au Ministère des Armées m'a permis d'acquérir des connaissances techniques militaires me permettant à présent d'offrir une réelle expertise à un potentiel employeur futur. De plus, mes compétences linguistiques en russe se sont considérablement améliorées, malgré l'absence de terrain. Enfin, J'ai eu l'opportunité de développer des compétences en OSINT, me permettant réellement de compléter ma formation initiale. Chaque enseignement dispensé par le Master ERPS m'a été utile au long de cette expérience professionnelle ; les concepts sociologiques propres à la zone ex-soviétique, les enjeux géopolitiques et les exercices de prospectives m'ont permis d'apporter une réelle plus-value appréciée par ma hiérarchie et ressentie dans mes productions. Cela m'a également permis d'établir des orientations possibles pour mon parcours professionnel futur.

Bibliographie

Sources académiques

Françaises

LIMONIER Kevin, AUDINET Maxime, *De l'enquête au terrain numérique : les apports de l'Osint à l'étude des phénomènes géopolitiques,* HERODOTE, 12/08/2022

https://www.herodote.org/IMG/pdf/limonier-audinet.pdf

LIMONIER Kévin, Comment l'OSINT est utilisé en géopolitique ?, Institut Français de Géopolitique, 19/07/2023

https://www.geopolitique.net/osint-geopolitique-kevin-limonier/

AUDINET, Maxime, Russia Today (RT) : Un media d'influence au service de l'Etat russe, Editions de l'INA, 2022, 192 p.

HOLEINDRE Jean-Vincent, Ce que la guerre fait aux sociétés, Dans La guerre (2014), pages 5 à 12

https://www.cairn.info/la-guerre--9782361062026-page-5.htm?contenu=article

MARCHETTI Dominique, Sociologie de la production de l'information, dans Écoles et "jeunes" dans les médias du Sud, 2002, pages 17 à 32

https://journals.openedition.org/cres/1653

GRANJON Fabien, Le FOULGOC Aurélien, Penser les usages sociaux de l'actualité, Dans Réseaux 2011/6 (n° 170), pages 17 à 43

https://www.cairn.info/revue-reseaux-2011-6-page-17.htm

TARRAGONI Federico, Chapitre 1. Le conflit comme fait social, Dans Sociologie du conflit (2021), pages 25 à 32

https://www.cairn.info/sociologie-du-conflit--9782200627270-page-25.htm

BURNIER Michel, Un nouvel activisme sur l'Internet ?, pages 103 -104, 2009

https://journals.openedition.org/terminal/2595?lang=en

Anglosaxonnes

MILLER, Daniel, (2018) 2023. "Digital anthropology". In The Open Encyclopedia of Anthropology, edited by Felix Stein. Facsimile of the first edition in The Cambridge Encyclopedia of Anthropology

https://www.anthroencyclopedia.com/entry/digital-anthropology

rapport de l'UNESCO, New Horizons in Digital AnthropologyInnovation for understanding humanity, Published in 2023 by the United Nations Educational, Scientific and Cultural Organization, 7, place de Fontenoy, 75352 Paris 07 SP, France and Splashlight Holding, LLC, 75 Varick Street, 3- FL. New York, NY 10013, USA

https://unesdoc.unesco.org/ark:/48223/pf0000382647

GLASSMAN Michael, KANG Min Ju, Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT), Computers in Human Behavior

Volume 28, Issue 2, March 2012, Pages 673-682

https://www.sciencedirect.com/science/article/abs/pii/S0747563211002585

HWANG Yong-Woon, LEE Yeong, KIM Hwankuk, LEE Hyejung, and KIM Donghyun, Current Status and Security Trend of OSINT, Hindawi, 18/02/2022

https://www.hindawi.com/journals/wcmc/2022/1290129/

STALDER Felix, HIRSH Jesse, Open Source Intelligence, First Monday, 2002

https://firstmonday.org/ojs/index.php/fm/article/download/961/882?inline=1

CAPPA Francesco, HAYES Darren R, Open-source intelligence for risk assessment, Business Horizon, 2018

https://www.sciencedirect.com/science/article/pii/S0007681318300296?casa_token=qG6oyvck91gAAAAA:pPTT5a7giiP-yS8cwcngX7FgeMhjOzV5kl02Pmde8jjAG4FkBjQL5kzy-LRDD6norJ3JlVGEnw

LOMAS Dan, The Death of Secret Intelligence? Think Again, Royal United Service Institute, 05/07/2023

https://rusi.org/explore-our-research/publications/commentary/death-secret-intelligence-think-again

BENES Libor, OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm, Journal of Strategic Security, Vol. 6, No. 3, Supplement: Ninth Annual IAFIE Conference: Expanding the Frontiers of Intelligence Education (Fall 2013), pp. 22-37 (17 pages)

https://www.jstor.org/stable/26485053?seq=1

LARUELLE, Marlène, Russia's Niche Soft Power Sources, Targets and Channels of Influence, IFRI, avril 2021

https://www.ifri.org/sites/default/files/atoms/files/laruelle_russia_niche_soft_power_2021.pdf

GALEOTTI, Mark, The Weaponisation of Everything: A Field Guide to the New Way of War, Yale, Yale University Press, 2022, 248 p.

https://www.cairn.info/revue-les-champs-de-mars-2021-2-page-205.htm

LARUELLE, Marlène, LIMONIER, Kevin, « Beyond "hybrid warfare": a digital exploration of Russia's entrepreneurs of influence », in Post-Soviet Affairs, vol. 37, n°4, 2021, p. 318-335.

https://www.researchgate.net/publication/353319539_Beyond_hybrid_warfare_a_digital_exploration_of_Russia's_entrepreneurs_of_influence

SZOSTEK, Joanna, « Nothing Is True ? The Credibility of News and Conflicting Narratives during « Information War » in Ukraine », in The International Journal of Press/Politics, 2018, vol. 23, n°1, p. 116-135.

https://eprints.gla.ac.uk/168622/

Jacobsen Lindskov Katja, Steinacker Karl, "Contingency Planning in the Digital Age: Biometric Data of Afghans Must Be Reconsidered", PRIO blog, 2021: consulté le 20/11/2023
https://blogs.prio.org/2021/08/contingency-planning-in-the-digital-age-biometric-data-of-afghans-must-be-reconsidered/

PALMIERI Paolo, Anonymity Networks and Access to Information During Conflicts: Towards a Distributed Network Organisation, 2016 8th International Conference on Cyber Conflict and Cyber Power, 2016, NATO CCD COE Publications, Tallinn

https://ccdcoe.org/uploads/2018/10/Art-16-Anonymity-Networks-and-Access-to-Information-During-Conflicts-Towards-a-Distributed-Network-Organisation.pdf

ETIENNE Hubert, The future of online trust (and why Deepfake is advancing it). AI Ethics 1, 553–562 (2021). https://doi.org/10.1007/s43681-021-00072-1

Nitschinsk, L., Tobin, S. J., Varley, D., & Vanman, E. J. (2023). Why Do People Sometimes Wear an Anonymous Mask? Motivations for Seeking Anonymity Online. Personality and Social Psychology Bulletin, 0(0).

https://journals.sagepub.com/doi/10.1177/01461672231210465

Russophones

ИГНАТОВА Анна Михайловна, ОТКРЫТЫЕ ДАННЫЕ КАК НОВЫЙ СПОСОБ ВЗАИМОДЕЙСТВИЯ ГОСУДАРСТВА И ОБЩЕСТВА, ГРАМОТА, 2015

https://www.gramota.net/articles/issn_1997-292X_2015_1-2_18.pdf

Дарменова Аида Советовна, Мамыкова Жанл Джумангалиевна, Андерсен Ким Норманн, ОТКРЫТЫЕ ДАННЫЕ: ДВАДЦАТИПЯТИЛЕТНЯЯ ИСТОРИЯ РАЗВИТИЯ, Экономика и бизнес, 2020

https://cyberleninka.ru/article/n/otkrytye-dannye-dvadtsatipyatiletnyaya-istoriya-razvitiya/viewer

Articles :

Français :

HOLEINDRE, Jean-Vincent, DOSSIER : LA GUERRE DE LA PRÉHISTOIRE À L'UKRAINE, La guerre, un fait social total, Hors-séries Sciences Humaines N° 27 - Octobre - novembre 2022

https://www.scienceshumaines.com/la-guerre-un-fait-social-total_fr_44974.html#:~:text=La%20guerre%20constitue%20une%20forme,un%20%C2%AB%20fait%20social%20total%20%C2%BB.

Anglosaxons :

KHALID Zaki, Social Sciences and Interdisciplinarity in OSINT Analysis, Medium, 9/12.2023 consulté le 04/04/2024

https://medium.com/@zakipantellica/social-sciences-and-interdisciplinarity-in-osint-analysis-644a8767b114

BBC News, What the leaked Pentagon documents reveal - 8 key takeaways, 15 April 2023, By Paul Adams, Jean Mackenzie and Antoinette Radford https://www.bbc.com/news/world-us-canada-65238951

The Conversation, Deepfakes in warfare: new concerns emerge from their use around the Russian invasion of Ukraine, Publié: 26 octobre 2023, 18:38

https://theconversation.com/deepfakes-in-warfare-new-concerns-emerge-from-their-use-around-the-russian-invasion-of-ukraine-216393

Ukrainiens :

Застосунок Резерв+ для військовозобов'язаних вже працює. Як завантажити, DW UA, 18 mai 2024

https://dev.ua/news/zastosunok-rezerv-dlia-viiskovozoboviazanykh-vzhe-pratsiuie-yak-zavantazhyty-1716006003?utm_source=tg&utm_medium=msg&utm_campaign=news_dev_ua_channel&utm_content=vzhe-pratsiuie

Contenu multimedia:

EURONEWS, Deepfake Zelenskyy surrender video is the 'first intentionally used' in Ukraine war, 16 mars 2022 consultée le 5/06/2024

https://www.youtube.com/watch?v=YkNKVAfA3_4