Les données de la guerre. *Big Data* et algorithmes à usage militaire

Article inédit, mis en ligne le 15 novembre 2018.

Olivier Koch

Olivier Koch est enseignant à l'Université Galatasaray dans le département de communication. Il est rattaché au laboratoire des Sciences de l'information et de la communication (LabSIC) de l'Université Paris 13. Ses travaux portent sur les enjeux de l'information dans des contextes de guerre et sur la réforme des médias en contexte de recomposition politique.

Plan de l'article

Introduction
Détecter et neutraliser
Prédire et anticiper les instabilités
« Economie de la promesse » (non tenue)
Conclusion
Références bibliographiques

Résumé

Les dispositifs « *Big Data* et algorithmes » ont été intégrés au secteur militaire américain dans les années 2000. En Afghanistan et en Irak, les armées les ont utilisés pour détecter les « insurgés » au sein de population et pour prédire de nouvelles « insurrections ». Ces dispositifs ont été employés dans le but d'automatiser la détection et la prédiction, et optimiser ainsi la prise de décision politique. Cependant, malgré les efforts institutionnels et financiers consentis, la promesse de doter le chef de guerre d'une ingénierie plus efficiente que les précédentes n'a pas été tenue. Et cet échec n'a pas remis en question la perpétuation de ces programmes. Nous proposons dans cet article d'analyser l'intégration des dispositifs « *Big Data* et algorithmes » au secteur militaire étasunien au prisme cette contradiction.

Mots clés

Big Data, contre-insurrection, comportements socioculturels, populations, prise de décision.

Title

Data of the war. *Big Data* and algorithms for military use

Abstract

The «*Big Data* and Algorithms» devices were integrated into the US military in the 2000s. In Afghanistan and Iraq, the armed forces used them to detect «insurgents» within the

population and to predict new «insurrections». These devices have been used to automate detection and prediction, thereby optimizing political decision-making. However, despite the institutional and financial efforts made, the promise to equip the warlord with more efficient engineering than the previous ones was not fulfilled. And this failure did not call into question the perpetuation of these programs. In this article, we propose to analyze the integration of «*Big Data* and Algorithms» devices with the US military sector through this contradiction.

Keywords

Big data, counterinsurgency, culture, sociocultural behavior, decision-making

Título

Los datos de la guerra. *Big Data* y algoritmos para uso militar

Resumen

Los dispositivos de «*Big Data* y algoritmos» se integraron en el sector militar americano en la década de 2000. En Afganistán y en Iraq, las fuerzas armadas los usaron para detectar «insurgentes» dentro de la población y predecir nuevas «insurrecciones». Estos dispositivos se han utilizado para automatizar la detección y predicción, optimizando así la toma de decisiones políticas. Sin embargo, a pesar de los esfuerzos institucionales y financieros realizados, la promesa de equipar al caudillo con una ingeniería más eficiente que las anteriores no se cumplió. Y este fracaso no cuestionó la perpetuación de estos programas. En este artículo, proponemos analizar la integración de los dispositivos de «*Big Data* and algoritmos» en el sector militar estadounidense a través de esta contradicción.

Palabras clave

Big Data, contrainsurgencia, cultura, comportamiento sociocultural, toma de decisiones

Introduction

« La culture est le "terrain humain" de la guerre, le terrain humain est le terrain clé »[1]. Cette déclaration du Major General Geoffroy Lambert restitue l'orthodoxie qui a guidé les réformes du secteur militaire étatsunien dans les années 2000. Durant cette décennie, les armées en Irak et en Afghanistan ont renoué avec la contre-insurrection, un art de la guerre dans lequel la détection des « insurgés » parmi le reste de la population est au centre des enjeux tactiques. Afin de s'orienter sur ce « terrain humain », le département de la Défense a investi dans le traitement automatisé de data sur les comportements socioculturels des populations autochtones. Les dispositifs « *Big Data* et algorithmes » ont ainsi été utilisés pour mener une guerre « centrée sur la culture » (Scale, 2004).

L'intégration de ces dispositifs au sein du secteur militaire étasunien fait l'objet de cet article. On se propose d'analyser ses formes et les logiques qui l'ont gouvernée à travers deux niveaux de ses manifestations concrètes. Tout d'abord, les programmes mis en œuvre pour guider les armées sur les terrains de la guerre irrégulière. Il s'agit, à ce pre-

.....

1. Cette citation est tirée de l'article de Yuri Lecchuk et d'Alexander Lubyansky, « Cultural agent model to predict inhabitant opinion réactions (CAMPHOR) : building and applying a dynamic humain terrain map », issu de la conférence « 13tgICCRTS C2 for complex behavior endeavor », [en ligne], Consulté le 2 février 2018, http://www.dodccrp.org/events/13th_iccrts_2008/CD/html/papers/156.pdf

mier niveau, de signaler quelles nouvelles technologies ont été incorporées aux systèmes de détection et de prédiction automatisées, avec quels effets de performance escomptés, puis de restituer leurs usages dans une économie du recours à la violence armée. A un deuxième niveau, l'intégration de ces dispositifs dans le secteur militaire est appréhendée à travers la réorganisation institutionnelle de la Recherche et Développement dont ont émergé les programmes. Cette réorganisation permet de saisir, en particulier, les dynamiques de convergences intersectorielles orchestrées au plus haut niveau de l'Etat fédéral.

La base documentaire exploitée dans cette investigation est composée de deux types de documents, différenciés par l'origine sectorielle de leurs auteurs. Une partie du corpus agrège des publications éditées par des organisations du département de la Défense. On a cherché à y relever les mobiles et les justifications du recours aux ingénieries des *data*. L'autre partie est composée de publications de chercheurs-ingénieurs en sciences computationnelles des données. Le travail de valorisation des performances de leurs recherches appliquées y a fait l'objet d'une attention particulière. En croisant les justifications des premiers et les valorisations des seconds, il s'agit de mettre en évidence la convergence de logiques d'acteurs — celles du politique (le chef des armées) et celles de l'ingénieur — sur un même horizon d'attente : l'optimisation de la prise de décision politique.

Cet article se compose de trois parties. La première porte sur la mise en œuvre de systèmes de détection du « terroriste » ou de l'« insurgé » au sein des populations afin de guider les drones vers leurs cibles. A l'aune de la réorganisation de la Recherche et Développement, la deuxième est consacrée à l'évolution des machines prédictives dédiées à l'anticipation des crises imminentes. Enfin, dans la dernière partie, on se propose de restituer les innovations technologiques de la guerre « centrée sur la culture » à partir d'une « économie de la promesse » (Joly, 2010), la promesse d'optimiser la prise de décision politique, puis de monter en quoi cette promesse n'est ni tenue, ni tenable.

Détecter et « neutraliser »

Depuis l'avènement de la cybernétique, l'informatique connectée a été employée pour parfaire les systèmes de guidage des armes vers leurs cibles (Forget, 2001). Avec le tournant contre-insurrectionnel en Irak, les dispositifs « *Big Data* et algorithmes » ont été employés à la détection des cibles humaines au sein des populations autochtones. Dans cette première partie, il s'agit d'analyser les modalités de fonctionnement et d'application de ces outils de détection en restituant leur emploi dans une économie du recours à la violence armée.

Comprendre le recours aux technologies de détection automatisée implique de saisir les spécificités de la guerre contre-insurrectionnelle. Dans ce type de conflit, l'ennemi se confond avec le reste de la population : il n'est pas nécessairement armé et en tenue militaire, et il évolue dans les milieux urbains comme d'autres citadins. De ce point de vue, la détection de l'« insurgé » dans le brouillard de la guerre irrégulière a deux enjeux concomitants. Au niveau tactique, il importe de repérer cet ennemi pour neutraliser ses capacités de résistance. Au niveau stratégique, l'enjeu est de le distinguer du reste des civils pour éviter de tuer des individus sans lien avec l'ennemi. Le risque serait d'accroître l'hostilité des populations vis-à-vis de l'occupation et de contribuer ainsi à la légitimation des groupes armés « insurrectionnels ». Or, de cette légitimité dépend le soutien des populations à ces groupes. Les dispositifs « *Big Data* et algorithmes » ont été utilisés dans les années 2000 pour modéliser les comportements de cet « insurgé » (ou « terroriste ») et pour optimiser ainsi la prise de décision du commandement.

Afin de parfaire cette modélisation, le département de la Défense a réorganisé ses activités en Recherche et Développement. En 2009, a été créé le *Human Social Culture Behavior program* (HSCB)[2] au sein duquel a été a été mis en œuvre le *Cultural Knowledge Consortium* (CKC). La mission de ce consortium était de développer des recherches en modélisation algorithmique des comportements socioculturels. A partir de 2010, le CKC est devenu le *Global cultural knowledge network* avec pour objectif de porter à une autre échelle la production et la coordination de ces savoirs. Cette organisation dont la mission est « *de rassembler toute la capacité intellectuelle des États-Unis [...] en guidant la connaissance socioculturelle vers la décision*[3] » est conçue comme l'infrastructure d'une communauté de recherche transnationale. Le secteur académique national a été également mis à contribution. Les dynamiques au sein des Universités ont été insufflées en 2008 par le projet *Minerva Research Initiative*, grâce à des financements visant à orienter les travaux en sciences sociales sur la cartographie-analyse de réseaux humains. Avec ces technologies de profilage des populations, déjà analysées par Armand Mattelart et André Vitalis (2014), une « nouvelle physique sociale » (Pucheu, 2017) de la déviance et du crime a vu le jour.

L'un des programmes les plus représentatifs de « la guerre centrée sur la culture » dans la deuxième moitié des années 2000 est le « *Human Terrain System* » (HTS) (« système du terrain humain »)[4]. Il est défini par ses entrepreneurs comme l'ensemble des « *éléments sociaux, ethnographiques, culturels, économiques et politiques des populations à travers lesquelles une force opère* », autant d'éléments qu'il s'agit de transformer en données numériques pour qu'elles soient « utilisées dans une partie du processus de prise de décision militaire » (Kipp *et al.*, 2006, p. 9). Le HTS est employé à la détection automatisée d'« insurgés » au sein des populations autochtones. Cette détection est fondée sur l'analyse comportementale d'individus appréhendés dans leurs réseaux affinitaires. Qui fait quoi ? Où ? Quand ? Et avec qui ? Voici en somme les principales questions auxquelles le système doit figurer les réponses sous formes de graphes. Selon la position nodale d'individus dans des réseaux estimés hostiles, leur « neutralisation » peut être décidée par les chefs de guerre, soit par mise à mort, soit par mise en détention.

Les informations et les data primaires (les inputs) du système sont collectées par observation humaine à travers des missions de renseignement —par des soldats et des anthropologues « *embedded* »— et à travers la surveillance automatisée des télécommunications locales et au moyen de caméras fixées sur des drones. Renseignement humain et renseignement automatisé sont ainsi conjugués dans la constitution des gisements de *data* exploités par le HTS. Les données de ces gisements, systématiquement enregistrées dans un *data center* aux Etats-Unis, sont combinées dans le but d'identifier des groupes et des « *ego networks* » dont le logiciel de *Mapping Human Terrain* (MAP-HT) produit la représentation. Cette cartographie sociale (le *output*) doit permettre aux armées de s'orienter dans le brouillard de la guerre irrégulière. Elle est constituée de trois calques superposés. Le premier calque figure des groupes et réseaux primaires définis selon des attributs qualifiés de « culturels » (dans le lexique des artisans du HTS) : religion, tribu, ethnie, clans. Le deuxième calque représente sous forme de graphe le « réseaux intégré » des relations de parenté, des relations affinitaires et des communications routinières entre individus. Enfin, à partir d'une fusion des deux premiers, le troisième calque superpose les graphes obtenus à la géographie physique des lieux grâce à un logiciel de géolocalisation.

.....

2. Cf. Human socio cultural behaviour modeling Program, [En ligne], Consulté le 19 juillet 2017, https://info.publicintelligence.net/DoD-SocioculturalBehavior.pdf

3. [En ligne]. Consulté le 25 juin 2017, https://community.apan.org/wg/oekn/

4. Mis en œuvre entre 2005 et 2006, officiellement le HTS aurait pris fin en 2014. Cependant, selon Benjamin D. Hopkins (2016), l'armée américaine a été contrainte d'avouer publiquement que le projet a été repris et intégré dans un nouveau programme de recherche (le Global Cultural Knowledge Network).

Le HTS schématise des « formes de vie » selon un procédé décrit par Grégoire Chamayou dans *Théorie du drone* (2016). Ces « formes » sont élaborées par l'analyse de données sur ce que font quotidiennement les individus dans leurs réseaux sociaux. De la récurrence de leurs activités émergent des patterns repérables (des «schémas de vie»). Au regard de ces récurrences,les comportements qui dévient de cette trame signalent une menace. Ces comportements déviants sont estimés en effet « signer » une appartenance à un réseau hostile, à un groupe d'« insurgés » ou une organisation « terroriste ». Dès lors, leur détection engage des « frappes par signature » *via* des drones, une mise à mort donc. Dans ce cas, la guerre cynégétique est avant tout une « chasse à l'homme» où, contrairement au modèle clausewitzien du duelliste, l'un des belligérants (le « terroriste ») ne se bat plus contre son adversaire : il devient une proie (*Ibid.*).

Le *Humain terrain system* a été utilisé dans la contre-insurrection en Irak et en Afghanistan, mais cette technologie est aussi devenue dans les années 2010 une pièce importante de la « guerre à distance » (« *remote warfare* »). Ce modèle opérationnel a servi de référence aux armées américaines et britanniques en Afrique, dans la lutte contre Aqmi et Boko Haram, et au Moyen-Orient dans la guerre contre l'«État islamique». Aux États-Unis, cette «guerre à distance» a singularisé les opérations militaires menées sous la présidence de Barack Obama (2009-2017), en rupture avec la logique d'occupation des territoires mise en œuvre en Irak sous le mandat de Georges W Bush (2001-2009). De ce point de vue, l'informationnalisation[5] de la guerre dans les années 2010 est au service d'une projection de la force sans déploiement d'hommes au sol. Des déploiements qui exposent les soldats au feu de l'ennemi et augmentent le nombre de « morts en opération », ce dont le gouvernant devrait rendre compte devant les publics domestiques. Les technologies de détection de la « guerre à distance » sont ainsi employées à la réduction des coûts politiques de la guerre.

Le dispositif contribue, sous un autre rapport, à l'économie du gouvernement des hommes dans les chaînes de commandement. L'automatisation de la détection transfère la responsabilité d'un interprète humain aux productions anonymes des graphologies numériques. Dans la concaténation des actes et des décisions qui mènent à la mise à mort, une partie de la responsabilité est ainsi déléguée aux machines détectives. Le commandement décide de l'exécution d'un homme, un soldat actionne le drone à distance derrière son écran mais, dans un cas comme dans l'autre, l'acteur est affranchi d'un travail d'interprétation des données (dont dépend l'imputation a posteriori des culpabilités liées aux crimes de guerre cynégétiques). Le dispositif permet de limiter ainsi les jugements que les différents opérateurs de la force armée pourraient prononcer sur l'usage de la violence « légitime » d'État. Or, ces jugements peuvent susciter chez ces opérateurs des hésitations, des refus d'obtempérer, et peuvent affecter ainsi la conduite de la guerre. La robotisation de la guerre sur les zones d'affrontement va dans le même sens. Elle pourvoit les armées de soldats-machines qui ne discuteront pas les ordres et qui ne refuseront jamais d'aller au combat (Singer, 2009). Sous ce rapport, l'intermittence homme-machine dans la division du travail militaire n'est pas seulement destinée à optimiser l'efficacité du déploiement de la force armée : elle agence le gouvernement des hommes.

Prédire et anticiper les « instabilités »

Conjointement au développement des machines détectives, le département de la Défense a financé la conception de programmes destinés à automatiser la prédiction de crises.

.....
5. L'« informationnalisation » de la guerre désigne le processus d'encodage d'existences et de pratiques qui entrent dans le périmètre de la rationalité stratégique.

Dans la lignée de systèmes mis en œuvre dans les décennies précédentes, l'objectif était de prédire des « instabilités » sociopolitiques et d'anticiper ainsi une reconfiguration des échiquiers géopolitiques. Dans cette deuxième partie, on se propose d'appréhender comment les machines prédictives ont évolué avec l'intégration des dispositifs «*Big Data* et algorithmes» dans le secteur militaire et, plus particulièrement, avec la redéfinition des enjeux stratégiques de la « guerre centrée sur la culture ».

Aux États-Unis, la « politique des oracles » est constituée en secteur professionnel depuis la guerre froide (Colonomos, 2014). Dans ce secteur, l'agence fédérale en charge du développement des nouvelles technologies à usage militaire (DARPA) a financé des systèmes de prédiction automatisée au milieu des années 1970, notamment dans le cadre du *Integrated Crisis Early Warning System* (ICEWS) (Andriole, Young, 1977). A suivre les analyses de Sean O'Brien (2002), à partir du milieu des années 1990 la prédiction automatisée s'est progressivement appuyée sur l'usage actuariel des sciences computationnelles et des algorithmes prédictifs. Conçu en 2005, le projet *Senturion* illustre cette évolution. Développé à l'Université de la défense nationale, il a été mis en œuvre dans le but de prédire les comportements de décideurs politiques (individus et groupes) dans des pays étrangers. Qui va faire quoi et avec quels effets ? Le programme répondait à ces questions en utilisant des *«data sur des échantillons de décideurs»*, et *«des algorithmes représentant des processus comportementaux »* (Abdollahian, Baranick, Efird, Kuger, 2006).

Un tournant a été amorcé dans la deuxième moitié des années 2000. La prédiction automatisée a été progressivement réorganisée selon les enjeux stratégiques de la « guerre centrée sur la culture ». Deux inflexions majeures marquent cette réorganisation. Le Integrated Crisis Early Warning System (ICEWS) qui avait vu le jour pendant la guerre froide a été intégré en 2009 au Human Social Culture Behavior program (HSCB). L'insertion du ICEWS dans le HSCB acte ainsi la volonté de l'administration américaine de faire évoluer les machines prédictives en exploitant des *Big Data* « socioculturelles ». Une seconde inflexion dans l'évolution des dispositifs prédictifs, consécutive à la première, s'est traduite par l'exploitation de ce type de data à partir de gisements de données issues des médias et des réseaux sociaux numériques (RSN). On se propose dans ce qui suit de restituer cette évolution à travers l'automatisation du codage des données médiatiques et l'exploitation des RSN dans le projet de Radar social.

Automatisation du codage des données médiatiques

La prédiction automatisée de crises exploite des « données d'événement » (« 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). L'analyse des contenus médiatiques doit permettre de saisir ce qui se passe dans différents pays (les « événements »). L'objectif est d'identifier les mutations des rapports de forces nationaux et subnationaux, de prédire et d'anticiper des « instabilités ». Avec l'insertion du ICEWS dans le HSCB, l'automatisation du codage de « données d'événements » serait passée à une autre échelle (Schrodt, Van Bracke, 2013). Les bases de données porteraient sur un nombre de pays plus important et exploiteraient bien davantage d'articles ou de reportages audiovisuels (175 pays et 20 millions de nouvelles en 2012) que les versions du même type précédemment mises en œuvre. La vitesse du codage automatisé aurait également sensiblement augmenté, au point de produire des données d'événements « presque en temps réel » (*Ibid.*, p. 25). Cette accélération permettrait de réduire au minimum le délai entre, d'une part, la fabrique des « *event data* » sur l'évolution des rapports politiques dans le monde et, d'autre part, la manifestation in situ de ces rapports quotidiennement relayés par les médias.

Volume de données et vitesse de traitement sont mis en avant par les artisans des programmes à l'adresse des politiques (*Ibid.* ; O'Brien, 2010). En valorisant la portée et l'effi-

cacité de ces technologies, il s'agit d'indiquer aux gouvernants américains qu'ils pourront optimiser leurs prises de décision. Dans la présentation de Philipp Schrodt et David Van Bracke (2013), un élément de ce travail de valorisation mérite une attention particulière. Les auteurs comparent à plusieurs reprises les performances de leurs systèmes aux capacités humaines, à leurs yeux sensiblement plus limitées. Cette comparaison peut être interprétée comme un travail de distinction élective dans le cadre d'une compétition intra-sectorielle. En effet, dans le secteur de la prédiction de crise, deux types de professionnels s'opposent au regard de leurs savoir-faire : le « *computational social scientist* » (le chercheur en sciences sociales computationnelles) et le « *political scientist* » (le politiste). Or, l'insistance avec laquelle les premiers soulignent les limites humaines des seconds (les politistes non-relégués par ordinateur) revient à disqualifier leurs compétences (estimées désormais obsolètes) et, ainsi, à délégitimer ces professionnels dans leurs prétentions à contribuer à la prise de décision politique.

Exploitation des RSN dans le projet de Radar social

Parmi les programmes développés dans le cadre du HSCB, le Radar social (« Social radar ») a été conçu comme un instrument de radiographie des mondes sociaux. Son système traite des données sur les émotions, les sentiments et les attitudes des populations civiles. L'ambition de ses concepteurs est de « détecter des signatures de comportements socioculturels » (HBSC, p. 47) et, par ce moyen, de prédire et d'anticiper l'émergence de conflits.

Ce « radar » exploite des gisements de data issues des médias (en utilisant les technologies de codage précédemment mentionnées) et des data extraites des réseaux sociaux numériques. Dans une présentation du projet de 2012, l'exploitation des RSN est davantage mise en exergue que dans la première présentation du projet datée de 2010 (Maybury, 2010). Cette attention est justifiée par la généralisation de leurs usages et l'ampleur des mobilisations qui s'y manifestent, les auteurs faisant explicitement référence aux mouvements protestataires du « printemps arabe » de 2011 et 2012 (Costa, Boiney, 2012). Or, ces mouvements n'ont pas été anticipés par l'administration de Barack Obama, alors même qu'ils ont contribué à reconfigurer les *statu quo* géopolitiques en Afrique du nord et au Moyen-Orient. Aussi, dans le but de mieux détecter et prévoir de tels mouvements civils, des outils destinés à faire émerger les principaux sujets dont discutent les internautes ont été intégrés à la seconde version du Radar social (2012), principalement en associant l'analyse de conversation et l'analyse de sentiments grâce aux techniques d'« *opinion mining* » (Shellman, Covington, Zangrilli, 2014). Les logiciels du Radar visent en effet à cartographier des « constellations de sentiments-cibles » (Costa, Boiney, 2012, p. 7) et, par géolocalisation, à associer ces données à des pays ou des régions. Le système doit permettre d'« identifier des points de rupture qui signalent des changements majeurs de sentiments susceptibles d'avoir des effets sur le comportement des populations ou des gouvernements » (*Ibid.*, p. 2). La détection de ces ruptures, et la prédiction des changements politiques conséquents, permettent en retour de mettre en œuvre des tactiques de propagande, de cyber-déception et des opérations psychologiques adaptées à ces évolutions. Elles entrent à ce titre dans la prise de décision politique.

Le Radar social poursuit les mêmes objectifs que les machines prédictives mises en œuvre dans les années précédentes : prédire les conflits. Cependant, ce à partir de quoi la prédiction automatisée est réalisée a sensiblement évolué avec ce programme et, plus généralement, avec l'insertion du ICEWS dans le HSCB. Dans la lignée des programmes développés dans les années 1990, le projet Senturion (voir supra), par exemple, était essentiellement focalisé sur les décideurs politiques. Le Radar social a changé le point de focale. Le système porte sur les manifestations de soutien ou d'aversion des populations

civiles vis-à-vis de ces décideurs. La recherche en modélisation computationnelle des comportements socioculturels organisée dans le cadre du HSCB est dévolue à ce déplacement d'objet. Les ingénieries algorithmiques sont développées pour automatiser l'indentification et la prédiction des liens entre gouvernés et gouvernants, entre suiveurs et leaders et, potentiellement, renforcer ou saper ce lien. Dans ce cas, les machines prédictives sont employées à la (re)configuration des environnements stratégiques civils dans lesquels la puissance américaine doit opérer.

Economie de la promesse (non tenue)

On se propose dans cette dernière partie de reconsidérer chaque dispositif sociotechnique précédemment présenté et de restituer leur développement dans l'« économie d'une promesse » (Joly, 2010). Il s'agira de montrer, dans un premier temps, en quoi la promesse d'une optimisation de la prise de décision politique grâce aux machines détectivo-prédictives n'est ni tenue, ni tenable. On se proposera, dans un second temps, d'interpréter le maintien de tels dispositifs malgré les déficiences de leur fonctionnement.

A suivre leurs artisans et leurs promoteurs, les technologies employées pour guider les drones vers leurs cibles permettraient de tuer exclusivement l'ennemi en le distinguant des civils innocents. Cependant, l'intensification du recours aux drones tueurs entre 2009 et 2013 n'a pas atteint ce but. Plusieurs études empiriques ont mis en avant la récurrence d'erreurs de ciblage causant la mort de civils sans lien avec les « terroristes » ou les « insurgés » (Aslam, 2014 ; Gil, 2014). Ces erreurs peuvent s'expliquer, d'abord, par la faiblesse des optiques utilisées sur les drones en altitude : les caméras embarquées ne permettent pas de distinguer distinctement les individus au sol. Elles peuvent s'expliquer, ensuite, par le fonctionnement de systèmes de détection qui associe un changement de comportement à une « déviance ». Afin de rendre évidents les travers de ce système, considérons l'exemple suivant : un homme en Irak n'est pas sympathisant de Daech mais son frère est combattant dans cette organisation. Ces deux frères ne se parlent plus depuis un certain temps. Leur mère décède. Pour organiser les funérailles ou pour se consoler mutuellement, le premier frère appelle régulièrement le second et le voit à plusieurs reprises. Ce changement le fera apparaître automatiquement dans le réseau « terroriste », comme un point nodal sur les graphes du contre-terrorisme. Dès lors, son exécution devient possible, voire nécessaire. Quoi qu'il en soit, les erreurs de ciblages et la mort de civils « innocents » créent de puissants ressentiments au sein des populations autochtones. Des ressentiments qui alimentent les sentiments hostiles vis-à-vis des Etats-Unis et qui nourrissent des processus dits de « radicalisation » (*Ibid.*). La promesse de l'optimisation de la violence armée « légitime » n'a pas donc pas été tenue, pourtant le recours aux machines détectives dans la guerre à distance a été maintenu dans les années 2010.

Avec l'automatisation du codage des « données d'événement » développée dans les années 2000, une autre promesse a été faite : celle d'une transparence de l'état événementiel du monde qui permettrait d'objectiver avec précision les rapports de force nationaux et subnationaux. Le codage automatisé « presque en temps réel » devait permettre d'optimiser la prise de décision politique en la dotant d'une nouvelle ingénierie prédictive. Cependant, la mise en représentation de ce monde au moyen d'*« event data »* issues des médias pose un certain nombre de difficultés qui ne sont pas considérées par les ingénieurs du codage. Lorsque ces ingénieurs envisagent les limites de leur système, la raison invoquée est que « *les nouvelles ne sont [...] qu'une fraction étroite de tous les événements qui ont lieu quotidiennement* » (Schrodt, Van Bracke, 2013, p. 25). L'argument porte sur le fait que la couverture médiatique des évènements est partielle. La partialité de cette couverture

dans la « fraction étroite » n'est pas quant à elle appréhendée. Pourtant, les travaux en sociologie du journalisme et en économie politique critique de l'information ont, de longue date, déconstruit l'idéal d'une représentation médiatique exacte et transparente du monde. Ces travaux ont montré notamment que le rôle des élites ou des grandes agences de presse internationales dans le fonctionnement des systèmes médiatiques a des effets conséquents quant à la *sélection* par les journalistes des événements et quant à leur *construction* (Stuart Hall *et al.*, 1978 ; Mattelart, 2016, 2017). Le projet d'identifier les rapports de forces nationaux et subnationaux à partir d'une analyse automatisée des médias se heurte à un autre obstacle. Dans de nombreux pays, les médias font l'objet d'un puissant système de contrôle. Or, ce contrôle permet de fabriquer des événements en conformité avec les lignes de la propagande nationale. Les tutelles sur les médias tunisiens sous le régime de Zine el-Abidine Ben Ali (1987-2011), par exemple, visaient (entre autre) à produire les représentations d'un pays stable, en mesure de rassurer les investisseurs internationaux. Aussi est-il bien hasardeux, au moyen du codage de nouvelles fabriquées dans ce type de dispositif de contrôle, de prédire quelque « instabilité » à venir.

En exploitant des données extraites des RSN, le Radar social est confronté à des difficultés similaires. Pour rappel, le Radar a été conçu pour prédire des révoltes et pour anticiper leurs conséquences géopolitiques. Afin de détecter en ligne des mouvements comme ceux du « printemps arabe », la version de 2012 du programme a intégré des outils d'analyse de conversation et d'*« opinion mining »*. Mais ces modifications ne changent rien quant à l'incapacité du système à remplir ses fonctions de prédiction. Le Radar social est inopérant parce que sa conception est emprunte d'un déterminisme technologique qui façonne une lecture erronée de l'histoire de ces mobilisations protestataires. En effet, si on prend pour exemple les révoltes en Tunisie et en Egypte en 2011, celles-ci ont commencé dans des régions intérieures déshéritées. Les réseaux sociaux numériques ont été l'une des arènes fragmentées où ces protestations se sont exprimées, mais les « révolutions » étaient déjà engagées. Il était donc impossible de prédire leur avènement à partir de ces réseaux. En somme, dans sa version de 2012, le Radar social a été façonné par la mythologie des «révolutions Facebook» ou « révolutions 2.0 », des révolutions qui n'ont pas eu lieu, et dont le principal travers consiste à surdéterminer le rôle qu'ont joué les réseaux sociaux dans la chute du régime de Zine el-Abidine Ben Ali ou d'Hosni Moubarak (Ferjani, Mattelart, 2011).

Les dispositifs de détection et de prédiction automatisées ne sont donc pas en mesure de tenir la promesse de leurs artisans-concepteurs, cependant chaque programme précité a été maintenu dans les années 2010. Plusieurs éléments peuvent être avancés pour interpréter la perpétuation de cette contradiction. Le travail promotionnel sur la performance des dispositifs, tout d'abord. Dans la littérature en Recherche et Développement appliquée aux usages militaires, des chiffres relatifs à la quantification de cette performance sont régulièrement avancés. La prédiction de crises des programmes développés dans le cadre de l'ICEWS, par exemple, est estimée fiable à 70 % (O'Brien, 2010 ; Schrodt, Van Bracke, 2013). Cependant, ce chiffre n'est appuyé par aucune preuve et les conflits « prédits » ne sont pas mentionnés. La précision quantifiée des machines détective est aussi fréquemment mise en avant, mais elle n'est pas balancée par les chiffres concernant les victimes de leur imprécision. Quoi qu'il en soit, ces chiffres ne sont pas réellement en mesure de « duper » les destinataires des services de détection et de prédiction. Aussi faut-il chercher le maintien de la contradiction à un autre niveau.

Derrière les promesses des ingénieurs se sont alignés les acteurs politiques et des capitaux importants. Cet alignement a eu un effet d'enrôlement sur d'autres secteurs dont on se bornera, ici, à indiquer quelques temps forts. Sous le mandat de Georges W. Bush, l'Etat fédéral a financé la recherche en *data mining*[6]. Au sein du complexe militaro-industriel —

dans le département de la Défense et chez les prestataires privés— les filières ont été réorganisées pour exploiter des data «socioculturelles» à des fins sécuritaires (Gonzales, 2010, 2015). De ce point de vue, l'administration de Barack Obama n'a pas marqué de rupture avec celle de son prédécesseur. Au contraire. Sous sa présidence, les data et leur traitement pour « gouverner à travers le pouvoir civil [7]» ont été placés au centre des réformes stratégiques en matière de diplomatie et de développement. Le *21st Century Statecraft* en 2009 a officiellement acté la volonté de cette administration de mettre à niveau les outils de la politique étrangère américaine en tirant profit des « réseaux » et d'un « monde interconnecté »[8]. A ces fins, l'État fédéral a financé la recherche en sciences du comportement appliquée au traitement des data. Ainsi, les acteurs de différents secteurs (industriel, politique, militaire, académique) se sont solidarisés sur l'horizon d'attente des promesses des dispositifs « *Big Data* et algorithme ». Dès lors, le maintien de programmes qui ne peuvent fonctionner à la hauteur de l'exactitude escomptée n'est plus si contradictoire qu'il y paraissait au premier abord. L'horizon d'attente n'appelle pas l'abandon de ces programmes mais, au contraire, leur perfectionnement. Les failles de la technologie sont appelées à être compensées par de nouvelles innovations tant que celles-ci concourent à la réalisation de la promesse. La prédiction de crise illustre cette logique : alors qu'elle est dite fiable à 70 % (sans preuve tangible), l'investissement est pourtant porté sur la correction des 30 % restants.

Conclusion

On a œuvré dans cet article à analyser l'intégration des dispositifs « *Big Data* et algorithmes » dans le secteur militaire au tournant de la guerre « centrée sur la culture ». Il ressort de cette investigation que les promesses de la détection et de la prédiction automatisées, au service de l'optimisation de la prise de décision politique, ont gouverné cette intégration. Nous avons souligné l'inefficacité des programmes mis en œuvre au regard des finalités que leur assignent leurs artisans-concepteurs. Afin de rendre compte de cette contradiction apparente, ont été esquissés les effets d'enrôlement entre acteurs de différents secteurs dans une « économie de la promesse » agencée au plus haut niveau de l'Etat fédéral. En guise de conclusion, on souhaiterait souligner que l'automatisation de la détection et de la prédiction doivent fonctionner avec des marges d'erreur. Ce déplacement de perspective implique de rappeler que l'incertitude est une condition du pouvoir de l'agir politique. En effet, si un homme politique n'a plus à interpréter, s'il doit exécuter ce que prédisent les machines, alors sa marge d'action est réduite à sa partie congrue. Plus les prédictions sont exactes, moins sa marge de manœuvre est importante. Autrement dit, la faillite des machines détectivo-prédictives est une condition de survie des professionnels de la politique. Raison pour laquelle, probablement, les politiques font preuve de tant de complaisance vis-à-vis des approximations des oracles mécanisés.

.....

6. Cf. United States Genaral Accounting Office, « Data mining. Federal efforts cover a wide range of uses », May 2004.

7. Cf. U.S. Departement of state, « Leading through civilian power : 2010 quadrennial diplomacy and developpement review », [en ligne], consulté le 19 février 2017, https://www.state.gov/documents/organization/153108.pdf

8. Cf. U.S. Departement of state, « 21st Century statecraft », [en ligne], consulté le 26 mars 2018, https://2009-2017.state.gov/statecraft/overview/index.htm

Références bibliographiques

Abdollahian, Mark ; Baranick, Michael ; Efird, Brian et Kugler, Jacek (2006), *Senturion : a predictive political simulation model*, Center for technology and national security policy national defense university, [en ligne], Consulté 19 septembre 2017, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA454175&Location=U2&doc GetTRDoc.pdf

Andriole, Stephen. J. et Young, Robert A. (1977), « Toward the development of an Integrated Crisis Warning System », *International Studies Quarterly*, n° 21, p. 107-150.

Aslam, Walid (2014), « Terrorist relocation and the societal consequences of US drone strikes in Pakistan», *The remote controle digest,* [en ligne], Consulté le 20 mars 2017, http://www.oxfordresearchgroup. org.uk/sites/default/files/Remote %20Control %20Digest.pdf

Chamayou, Grégoire (2016), *Théorie du drone,* Paris : La fabrique.

Colonomos, Ariel (2014), *La politique des oracles. Raconter le futur aujourd'hui*, Paris : Albin Michel (collection « Bibliothèque des Idées »).

Costa, Barry et Boiney, John (2012), *Social radar, Mitre Corporation*, [en ligne], consultée le 26 juin 2017, https://www.mitre.org/sites/default/files/pdf/12_0581.pdf

Ferjani, Riadh, Mattelart, Tristan (2011), « Monde arabe : les révolutions 2.0 n'ont pas eu lieu », *Médias*, n° 30, p. 67-94.

Forget, François (2001), « Réseaux d'informations et mutations stratégiques », *Panoramiques*, p. 65-78.

Gill, Paul (2014), « The impact of drone attacks on terrorism : the case of Pakistan », *The remote controle digest*, [en ligne], Consulté le 20 mars 2017, http://www.oxfordresearchgroup. org.uk/sites/default/files/Remote %20Control %20Digest.pdf

Gonzales, Roberto J. (2010), *Militarizing Culture,* Walnut creek : Left coast press.

Gonzales, Roberto J. (2015), « Seeing into hearts and minds, Part 1 », *Anthropology today*, n° 31, p. 8-18.

Hall, Stuart ; Critcher, Chas ; Jefferson, Tony, Clarke, Jhon et Roberts, Brian (19878), *Policing the crisis : Mugging, the State, and Law and Order,* Londres : Palgram Macmillan.

Hopkins, Benjamin D. (2016), « The longue durée of Human Terrain : politics, cultural knowledge and the technical fix », *Anthropology today*, n° 32, p. 8-12.

Joly, Pierre-Benoit (2010), « On the economics of technoscientific promises » (p. 203-222), in Akrich, Madelein ; Barthe Yannick ; Muniesa, Fabian ; Mustar, Philippe (dir.), *Débordements : mélanges offerts à Michel Callon*, Paris : Presse des Mines.

Kipp, Jacob ; Grau, Lester ; Prinslow, Karl et Smith, Don (2006), « The Human Terrain System : a CORDS for the 21st Century », *Military Review*, n° 86, p. 8-15.

Mattelart, Armand ; Vitalis, André (2014), *Le profilage des populations, du livret ouvrier au cybercontrôle*, Paris : La découverte.

Mattelart Tristan (2016), «Déconstruire l'argument de la diversité de l'information à l'heure du numérique : le cas des nouvelles internationales», *Les Enjeux de l'Information et de la Communication*, n° 17/2, 2016, p. 113 à 126, consulté le lundi 5 novembre 2018, [en ligne] URL : https://lesenjeux.univ-grenoble-alpes.fr/2016/dossier/07-deconstruire-largument-de-diversite-de-linformation-a-lheure-numerique-cas-nouvelles-internationales/

Mattelart, Tristan (2017), « Les enjeux de la circulation transnationale de l'information : des agences de presse aux plateformes du web », in Koch, Olivier et Mattelart, Tristan

(dir.), *Géopolitique des télévisions transnationales d'information*, Paris : Mare & Martin.

Maybury, Mark (2010), «Social radar for smart power» (p. 26-36), in Schmorrow, Dylan et Nicholson, Denise (éd.), *Cross-cultural decision making*, New York : Taylor & Francis group.

O'Brien, Sean (2002), « Anticipating the good, the bad, and the ugly : an early warning approach to conflict and instability analysis », *The journal of conflict resolution*, vol. 46, n° 6, p. 791-811.

O'Brien, Sean (2010), « Crisis early warning and decision support : contemporary approaches and thoughts on future research », *International studies review,* vol. 12, n° 1, p. 87-104.

Pucheu, David (2017), « Social *Big Data*. Le phantasme d'une nouvelle physique sociale », *Etudes digitales,* vol. 2, n° 2, p. 89-106.

Schrodt, Philipp A. ; Van Bracke, David (2013), « Automated coding political event data » (p. 23-49), in Subralmanian, V.S. (éd.), *Handbook of computational approaches to counterterrorism*, New York : Springer science.

Shellman, Steve ; Covington, Michael et Zangrilli, Marcia (2014), « Sentiment & discourse analysis : theory, extraction, and application », *Socio-Cultural Analysis with the Reconnaissance, Surveillance, and Intelligence Paradigm,* [en ligne], Consulté le 13 février 2018, http://nsiteam.com/social/wp-content/uploads/2016/01/Socio-Cultural-Analysis-with-the-Reconnaisance-Surveillance-and-Intelligence-Paradigm.pdf

Singer, Peter (2009), *Wired for war. The robotics revolution and conflict in the 21st Century,* New York : Penguin books.