Guerre de l'information, guerre hybride… ces termes sont utilisés pour redéfinir ce que sont devenus les conflits du 21e siècle. Les moyens ont changé, mais les objectifs restent les mêmes : imposer sa volonté que cela soit par la force, la persuasion ou la déstabilisation politique.

Intelligence économique

Guerre de l'information et politique : Quelles conséquences pour la sécurité de la Suisse ?

Kilian Cuche
Collaborateur scientifique à la chaire Economie de Défense de l'Académie militaire (ACAMIL) à l'EPF de Zurich

« *Le combattant qui l'emporte est celui qui gagne la campagne de l'information. Nous en avons fait la démonstration au monde : l'information est la clef de la guerre moderne – stratégiquement, opérationnellement, tactiquement et techniquement.* »
Cette citation de Glenn K. Otis (1929-2012), général quatre étoiles américain, illustre parfaitement la place stratégique que l'information a prise dans les conflits contemporains, et par extension dans toute la société.

La maîtrise de l'information confère un avantage stratégique sur l'adversaire en tirant parti d'une asymétrie de l'information. Elle aide à sortir vainqueur des conflits et est devenu un enjeu capital dans les conflits du 21ème siècle. Toutefois, ces principes ne sont pas nouveaux. En effet, le stratège et général chinois Sun Tzu préconisait déjà à son époque de soumettre son ennemi sans combattre : « *Il faut plutôt subjuguer l'ennemi sans donner bataille : ce sera là le cas où plus vous vous élèverez au-dessus du bon, plus vous approcherez de l'incomparable et de l'excellent.* »

En parallèle de ces nouvelles formes de conflits, le développement des technologies de l'information et de la communication (TIC) ainsi que l'influence qu'ont pris les médias de masse dans la société ont fondamentalement modifié les comportements humains face à l'information. Bien que le facteur humain ne puisse jamais être remplacé complétement par les TIC, ces dernières sont exploitées et mises en œuvre afin de préparer le terrain et gagner des objectifs stratégiques. Ces actions sont appelées plus communément « opérations d'informations ».[1]

La guerre de l'information n'est cependant jamais menée seule car elle est accompagnée d'actions sur le terrain et elle se concrétise sous une forme de « guerre hybride ». Le général russe Valery Gerasimov a théorisé ces concepts dans sa doctrine et a ainsi démontré l'importance croissante des moyens non-militaires pour atteindre des objectifs stratégiques. Cette doctrine a principalement été mise en pratique lors des événements survenus en Ukraine en 2014. Les analystes ont donc pu constater que la maîtrise de l'information, les actions de communication et les opérations d'informations ouvrent des possibilités asymétriques pour réduire le potentiel de l'adversaire et influencer les structures étatiques et la population ainsi que sortir vainqueurs des différentes compétitions.[2] Dernièrement, le Conseil fédéral a souhaité l'adaptation des moyens de l'armée suisse afin de pouvoir répondre à ces nouvelles formes de conflits.[3]

Bien qu'utilisée principalement dans des actions militaires, la guerre de l'information et ses principes peuvent également être appliqués à d'autres domaines, notamment celui de la politique. En effet, selon Clausewitz, la guerre est uniquement la continuation de la politique par d'autres moyens. Il existe également une compétition entre les partis politiques pour faire triompher leurs idées de même que leurs candidats face au peuple et à leurs adversaires au niveau de la politique nationale. A l'international, les États ont également parfois des intérêts à faire valoir et ces derniers peuvent les imposer de manière détournée au moyen de campagnes d'influence. L'information est donc, ici aussi, une des clés, si ce n'est *la* clé du succès.

TIC et influence politique

La communication d'influence et les manipulations politiques se développent également de plus en plus grâce aux TIC. La multiplication des sources de données (réseaux sociaux, sondages en ligne, bases de données…) fournit de plus en plus d'informations aux stratèges politiques afin de mener à bien une campagne politique,

2 https://www.lettrevigie.com/blog/2015/04/24/guerre-hybride-ou-doctrine-gerasimov/

3 https://www.24heures.ch/suisse/L-armee-doit-se-preparer-a-des-conflits-hybrides/story/17369839

une élection ou une campagne d'influence. En réalité, des techniques d'analyses du *Big Data* ont été utilisées dans plusieurs campagnes récentes et certaines techniques de la guerre de l'information sont de plus en plus utilisées dans des campagnes d'influence.

On peut citer l'A*stroturfing*[4] qui désigne le fait de donner l'apparence d'un phénomène de masse sur internet à un phénomène en réalité créé de toutes pièces pour influencer l'opinion publique. Ces méthodes sont principalement utilisées dans un cadre d'influence politique. En effet, selon une étude, la mise à l'agenda politique semble être la fonction prépondérante des stratégies d'Astroturfing.[5] Le réseau social Twitter est particulièrement utilisé pour les actions d'Astroturfing en raison de sa portée et de la rapidité à laquelle sont transmises les informations sur ce réseau.[6] En Suisse, une utilisation de faux comptes ou « robots » a été détectée sur le réseau social *Twitter* à l'occasion de la campagne de votation sur l'initiative No Billag.[7]

Également les actions de *Soft Pow*er[8] qui sont en fait la capacité d'influence et de persuasion d'un État, d'une société, d'une ONG ou d'un groupe minoritaire auprès d'autres acteurs pour les conduire à penser de la même façon que lui ou à changer le comportement de manière indirecte, en douceur, sans que ces autres acteurs aient l'impression d'y avoir été contraints. Par exemple, la production culturelle d'un pays est un outil majeur du *Soft Power* avec sa capacité de changer la perception des gens sur une thématique. La représentation de l'armée américaine a largement été influencée par les nombreux films hollywoodiens tels que *Top Gun, Apocalypse Now* ou encore *Full Metal Jacket* pour ne citer que les plus connus. Dans cette pratique aussi, les TIC ont fondamentalement changé la donne en apportant la puissance des réseaux et la révolution du web 2.0 et des réseaux sociaux qui permettent de distiller des messages au plus grand nombre afin d'influencer sur les façons de penser à long terme.

L'OTAN a ajouté le terme de « guerre hybride » à son vocabulaire depuis l'intervention des forces spéciales russes en Crimée et son annexion par la Russie en 2014.

4 https://www.lesinrocks.com/2017/02/06/actualite/fake-manipulations-reseaux-sociaux-faut-vite-comprendre-quest-lastroturfing-11910209/

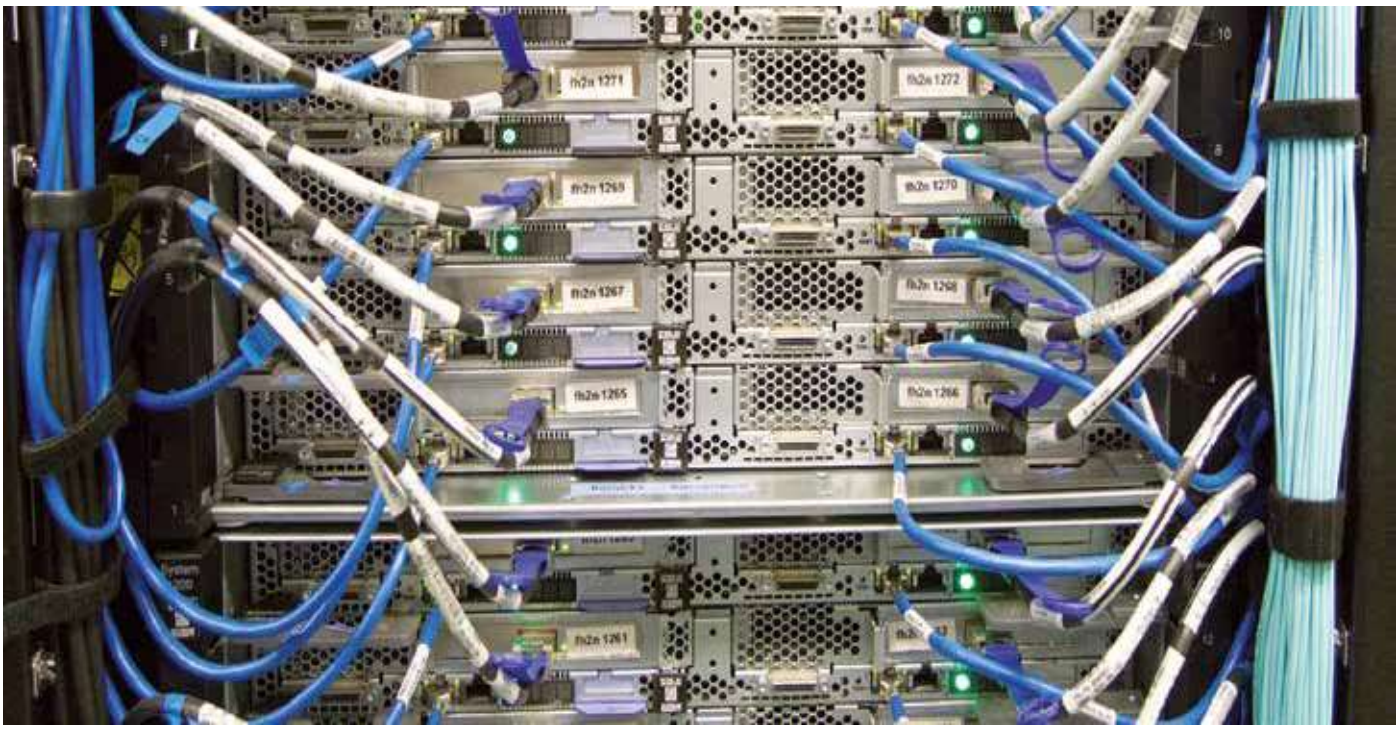
5 http://journals.openedition.org/communiquer/487

6 https://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/viewFile/2850/3274

7 https://www.aargauerzeitung.ch/leben/digital/abstimmungskaempfe-via-twitter-manipulieren-das-schafft-sogar-ein-laie-132397676

8 http://www.toupie.org/Dictionnaire/Soft_power.htm

Il est nécessaire de se rappeler que toutes les actions qui se passent sur le web sont en réalité des données transférées par des câbles physiques. Ces derniers représentent un véritable enjeu de souveraineté numérique.



Ces méthodes, couplées à la multiplication des *Fake News* sur internet ainsi qu'à l'isolement des internautes dans des bulles de filtres[9] et des chambres d'échos[10] offrent de nouvelles possibilités pour la communication d'influence.[11] Comme on a pu le constater, *Facebook* a récemment été impliqué dans plus d'une soixantaine de cas d'ingérence politique, notamment le scandale Cambridge Analytica qui a fait grand bruit.[12]
Dans ce contexte de surcharge informationnelle désorganisée et influencée, les politiciens sont de plus en plus vulnérables aux attaques informatiques et aux campagnes d'influence. Ces derniers étant impliqués dans des processus décisionnels concernant la sécurité de la Suisse et le développement de ses forces armées, il est urgent de les sensibiliser aux dangers potentiels apportés par ces nouvelles menaces qui sont également citées comme thèmes principaux dans le dernier rapport du SRC sur la sécurité de la Suisse.[13]

Risques pour la sécurité de la Suisse

Ces menaces sont donc bien réelles et n'appartiennent plus au domaine de la fiction ou des théories complotistes. En effet, on entend de plus en plus fréquemment dans les médias que des campagnes d'influence ou de désinformation (souvent en provenance de la Russie, mais pas que!) ont encore frappé sur tel ou tel sujet politique.
En mai 2019, la chaîne d'état russe *Russia Today* a été soupçonnée d'être à l'origine d'une campagne de désinformation sur la technologie 5G.[14] De plus, les autorités européennes ont également détecté une "activité de désinformation continue et soutenue de la part de sources russes" lors des élections européennes, visant à influencer les électeurs et à décourager leur participation, selon un rapport de la Commission européenne.[15]

On peut donc imaginer que des acteurs étatiques ou privés qui ont des intérêts à faire valoir concernant la politique de sécurité de la Suisse peuvent utiliser ces techniques d'influence afin de faire pencher la balance en leur faveur. L'introduction de la technologie 5G peut radicalement changer les méthodes de communication des forces armées et cette dernière doit être décidée politiquement. C'est également le cas du choix du nouvel avion de combat qui est une véritable guerre d'influence pour savoir qui sortira vainqueur de l'appel d'offres.[16] En effet, on peut penser que certains acteurs préfèreront le choix d'un avion plutôt qu'un autre que cela soit pour des raisons tant économiques que stratégiques.

Les budgets militaires sont également votés par le parlement et ils déterminent fortement les possibilités et les capacités de l'armée suisse. De plus, certaines votations concernant l'armée sont directement soumises au peuple (Gripen, initiatives du GSSA…) et pourraient potentiellement subir des campagnes d'influence afin d'atteindre un résultat qui affaiblirait les forces armées et par conséquent, la sécurité de la Suisse.

L'Intelligence Economique pour minimiser les risques

Mais alors que faire pour se protéger, et particulièrement les personnes impliquées dans des processus décisionnels critiques. Il existe une discipline appelée Intelligence Economique (IE) qui permet de réduire les risques en appliquant ses principes fondamentaux.

L'IE consiste en la maîtrise, la protection et l'exploitation de l'information afin de comprendre et anticiper l'environnement extérieur, les acteurs, les risques et les opportunités. Ceci dans le but de protéger le patrimoine informationnel et stratégique et d'agir sur les bons leviers d'influence. Le tout dans le respect des règles et avec l'utilisation de sources ouvertes contrairement à l'espionnage industriel. On peut définir l'IE avec trois piliers : la veille, la protection et l'influence.

Le premier pilier de l'IE est la veille. Cette dernière est basée sur le cycle du renseignement et consiste concrètement en la détection des besoins en information, la collecte de l'information, l'exploitation de l'information collectée et sa diffusion.

En effet, au travers de la veille, la personne impliquée peut capitaliser les informations stratégiques dont elle a besoin pour ses actions de communication d'influence ainsi qu'identifier les campagnes d'influence de l'adversaire. Elle peut également protéger ses informations stratégiques avec l'aspect protection de l'IE dans le but de se prémunir des actions de guerre de l'information et de déstabilisation la visant.

Un bon processus de veille permet d'obtenir les bonnes informations, vérifiées et analysées afin de ne pas succomber aux actions d'Astroturfing ou de Fake News. Par exemple, une personne mal renseignée pourrait baser son argumentaire sur une Fake News ou une fausse mobilisation de l'opinion publique mise en avant par une campagne d'Astroturfing et se décrédibiliser lors de son discours. Une bonne analyse de l'environnement permet également d'identifier quels acteurs pourraient effectuer des actions d'influence contre le parti ou le politicien ce qui lui permettrait de s'en prémunir ou de les détourner avant qu'il ne soit trop tard.

9 https://www.letemps.ch/culture/lere-linformation-fragmentee-jugement-mene-bout-nez

10 http://arxiv.org/abs/1801.01665

11 https://www.letemps.ch/opinions/federalisme-meilleur-antidote-contre-manipulations-politiques

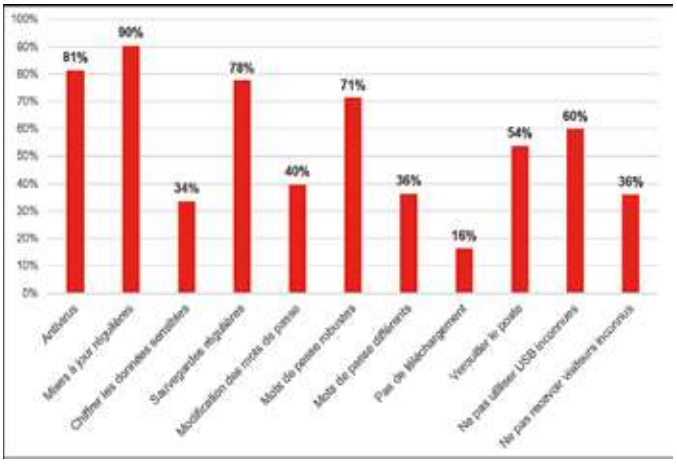
12 https://www.republik.ch/2018/05/16/facebook-influenced-elections-in-66-countries

13 https://www.newsd.admin.ch/newsd/message/attachments/57074.pdf

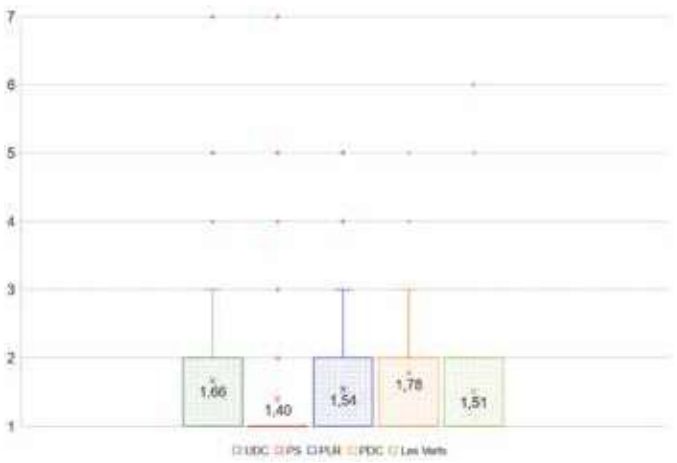
14 https://www.rts.ch/play/radio/forum/audio/la-chane-detat-russe-russia-today-serait-a-lorigine-dune-campagne-de-desinformation-sur-la-5g-aux-usa?id=10414970

15 https://www.rts.ch/info/monde/10507126-des-sources-russes-auraient-tente-d-influencer-les-elections-europeennes.html

16 https://www.24heures.ch/suisse/Qui-va-gagner-les-milliards-de-la-grande-bataille-du-ciel/story/16115920



Pratiques de protection des informations effectuées par la classe politique au niveau suisse. Enquête réalisée en 2018, envoyée à tous les parlementaires fédéraux et cantonaux avec un taux de réponse de 17 % qui équivaut à 532 réponses.



Niveau de familiarité avec l'Astroturfing au niveau suisse. La moyenne est très basse et se situe entre les réponses « pas du tout familier » et « peu familier » avec le sujet. Les réponses proviennent de la même enquête que citée plus haut.

Concernant la protection des informations, il peut être judicieux de mener un audit de sûreté dont le but est d'identifier les menaces, d'évaluer les opportunités d'occurrence de ces dernières ainsi que de découvrir les vulnérabilités existantes.

Dans un contexte politique, il s'agirait donc de faire un état des lieux des menaces pour les élu(e)s et d'imaginer la probabilité que celles-ci se produisent afin d'allouer les bonnes ressources pour les actions de protection ainsi que d'identifier les vulnérabilités existantes afin de les combler pour ne pas subir une fuite d'informations et mettre ainsi en danger le patrimoine informationnel ou une campagne d'influence.

De plus, les bonnes pratiques élémentaires de sécurité informatique (mises à jour régulières, sauvegardes, chiffrement des données sensibles, mots de passe robustes…) sont également de mise afin de minimiser les risques.

La sensibilisation comme moyen d'action

Les techniques les plus élaborées telles que l'Astroturfing ou la création de *Fake News* ainsi que leur propagation grâce à des algorithmes d'intelligence artificielle sont encore peu connues alors que ces dernières sont les plus dangereuses en ce qui concerne les ingérences politiques. Il reste donc encore un grand travail de sensibilisation à faire concernant l'usage des nouvelles technologies et leur impact sur les processus décisionnels.

La sensibilisation des élus et des personnes impliquées dans des processus décisionnels critiques pour la sécurité est donc indispensable afin de minimiser les risques de subir une campagne d'influence. Cette idée a d'ailleurs été récemment proposée par des représentants bipartisans aux Etats-Unis dans l'objectif de faire passer un entraînement annuel de cybersécurité aux membres du congrès.[17] C'est une nécessité primordiale afin de garantir un niveau de protection minimal car comme le révèle un récent rapport, les partis politiques américains et européens ont encore des problèmes concernant la cybersécurité.[18]

Cette prise de conscience est également présente dans le monde des entreprises et des administrations. En Suisse, les employés de la Confédération doivent passer un test de sécurité intégrale comprenant un volet *cyber* chaque année. Dans les entreprises, la thématique de la cybersécurité prend de l'ampleur et la sensibilisation est l'un des éléments principal.[19]

Pour terminer, précisons que cet article a largement été inspiré par les résultats du travail de Bachelor intitulé « Intelligence Economique et politique: besoins et pratiques dans les principaux partis politiques suisses» que nous vous invitons à consulter intégralement en ligne.[20]

K. C.

17 https://www.securitymagazine.com/articles/90291-cybersecurity-education-for-congress-members?v=preview

18 https://www.wired.com/story/political-parties-cybersecurity-hygiene-problems/

19 https://www.cvci.ch/fileadmin/documents/cvci.ch/pdf/Medias/publications/divers/12315_ENQUETE_CYBERSECURITE_PROD_PP.pdf

20 Ce travail de Bachelor a reçu le prix à l'Innovation 2018 de la HES-SO, HEG Genève, récompensant un travail innovant dans le domaine « économie et services » https://doc.rero.ch/record/323603?ln=fr

De la Chine à la Suisse, le recours aux technologies à base d'intelligence artificielle suscite à la fois fascination et inquiétude. Que la reconnaissance faciale soit un instrument de surveillance ou de protection de la population dans l'espace publique, celle-ci apparaît comme un outil de renseignement. À ce titre, l'essentiel n'est-il pas de trouver et de maintenir, à l'exemple de Genève, un équilibre entre les exigences de sécurité et celles liées à la sphère privée ?

Intelligence économique

La reconnaissance faciale comme nouvel outil de renseignement ?

Ataa Dabour
Présidente fondatrice, Security & Human Rights Association - SHR

L'emploi de l'intelligence artificielle (IA) basé sur le *machine learning* et le *deep learning* a connu une montée en puissance considérable ces dernières années. Les algorithmes se chargent désormais de l'analyse de données avec une précision jamais vue. La révolution de l'IA est en grande partie « une révolution de la perception des machines et de leur capacité à traiter des informations complexes. »[1]

Outre la voix, l'empreinte digitale, et le scan rétinien, la reconnaissance faciale figure parmi les technologies qui ont réalisé une très forte progression. L'application possible de la reconnaissance faciale à la fois au domaine militaire et au domaine civil fait de cette technologique une technologie à double usage. Autrement dit, il s'agit d'une *dual-use technology*. C'est l'emploi de la reconnaissance faciale à usage civil justifié par des raisons sécuritaires qui nous intéresse, dans un contexte où la surveillance et le renseignement sont en plein boom.

Reconnaissance faciale à usage civil

Partout où le recours à la reconnaissance faciale est d'usage, celui-ci suscite des questions relatives à la protection des données, aux droits humains et à l'éthique. Cette technologie est- elle employée à des fins de surveillance et de renseignement ou à des fins de protection de la population et de lutte contre la criminalité ?

Avec 176 millions de caméras nourries à l'intelligence artificielle déjà installées en 2016, et trois fois plus prévues d'ici à 2020,[2] la Chine représente le marché de surveillance le plus dynamique du monde. Avec son dernier programme en date, *Xue Liang* - Œil de Lynx,[3] le gouvernement chinois a pour but d'élargir davantage le réseau de surveillance du pays. A terme, la collecte de données recueillies sur sa propre population servira à établir un système global d'identification informatisé et connecté aux fichiers des forces de l'ordre.

Le système chinois de récolte d'information et de surveillance par des caméras dites intelligentes a poussé la Grande-Bretagne, notamment Londres, à réfléchir à la mise en place d'un système quasi similaire. Depuis 2016, des caméras dotées de reconnaissance faciale ont été installées dans plusieurs quartiers de Londres. Les tests menés par la capitale britannique visent à identifier des personnes recherchées par les forces de l'ordre et réduire la violence.

Face à ce développement, la directrice de *Big Brother Watch* (BBW), Mme. Silkie Carlo n'a pas manqué de souligner combien « l'utilisation par la police de cet outil de surveillance autoritaire en l'absence totale de base légale ou démocratique est alarmante. »[4] Cela d'autant plus qu'il semblerait que les tests menés par la police métropolitaine de Londres entre 2016 et 2018 indiquent que 80 à 90 %[5] des suspects signalés par cette technologie sont innocents.
La France, l'un des pays champions des technologies numériques de surveillance, suit également le même développement. En effet, le ministère de l'intérieur français, Mr. Gérard Collomb, annonçait en 2018 la nécessité de l'emploi de la reconnaissance faciale

2 Bostra, Rosa, « La reconnaissance faciale se répand en Chine, » Le Temps, 10 Janvier 2018. (https://www.letemps.ch/economie/reconnaissance-faciale-se-repand-chine).

3 Li, Sharon, « Eye Spy: Chinese Surveillance and the Dawn of Digital Authoritarism, » China Hands, 20 Janvier 2019. (https://chinahandsmagazine.org/2019/01/20/eye-spy-chinese-surveillance-and-the-dawn-of-digital-authoritarianism/).

4 « À Londres, la police teste la reconnaissance faciale pour détectées des personnes recherchées, » NextInpact, 18 Décembre 2018. (https://www.nextinpact.com/brief/a-londres--la-police-teste-la-reconnaissance-faciale-pour-detecter-des-personnes-recherchees-7126.htm).

5 Lefebre, Arnaud, « Le logiciel de reconnaissance faciale des policiers de Londres se trompe dans 96 % des cas, » Express Business, 16 Mai 2019. (https://fr.express.live/le-logiciel-de-reconnaissance-faciale-des-policiers-de-londres-se-trompe-dans-96-des-cas/).