Mondialisation.ca
Centre de recherche sur la mondialisation

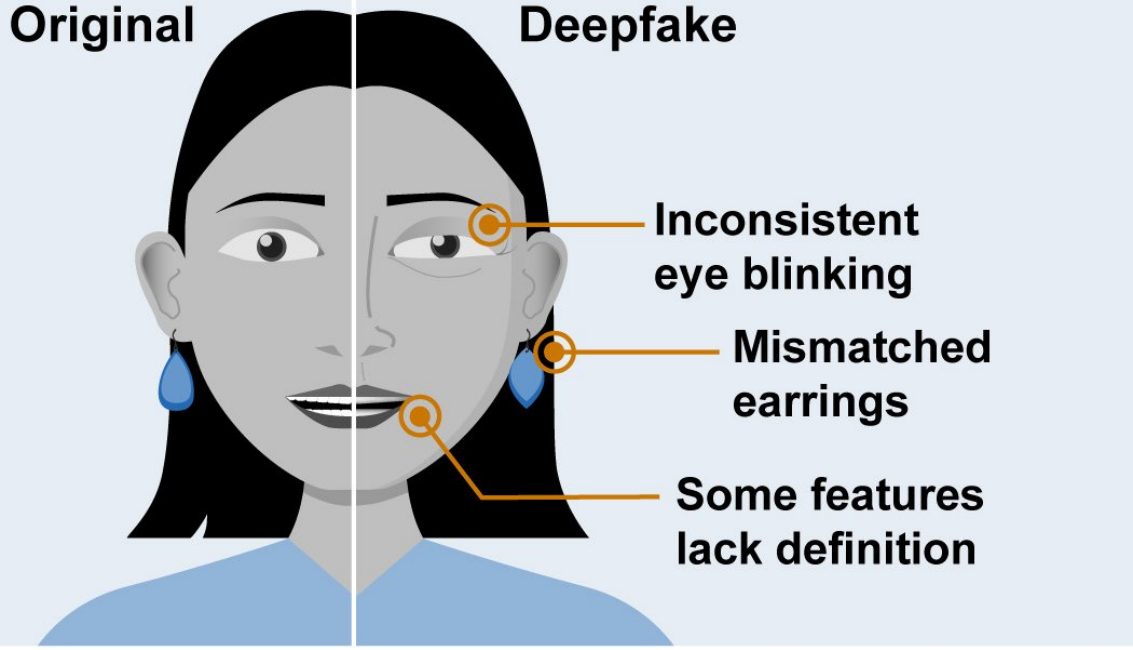
Les Forces spéciales étasuniennes veulent utiliser les « deep fakes » pour mener des opérations psychologiques

Par Sam Biddle
Mondialisation.ca, 24 mars 2023
The Intercept 6 mars 2023

Thème: Désinformation médiatique, Guerre USA OTAN, Services de renseignements

L'U.S. Special Operations Command (SOCOM), responsable de certaines des activités militaires les plus secrètes du pays, se prépare à mener des campagnes de propagande et de tromperie sur Internet en utilisant de fausses vidéos, selon des documents contractuels fédéraux examinés par *The Intercept*.

Ces plans, qui décrivent également le piratage d'appareils connectés à l'internet pour les écouter afin d'évaluer la sensibilité des populations étrangères à la propagande, interviennent à un moment où le monde entier débat intensément des campagnes de « *désinformation* » technologiquement sophistiquées, de leur efficacité et de l'éthique de leur utilisation.



Alors que le gouvernement américain met régulièrement en garde contre le risque de « *deep fakes* » et travaille ouvertement à la mise au point d'outils pour les contrer, le document du commandement des opérations spéciales, ou SOCOM, constitue un cas presque sans précédent où le gouvernement américain signale ouvertement son désir d'utiliser cette technologie très controversée de manière offensive.

Les aspirations du SOCOM en matière de propagande de nouvelle génération sont décrites

dans un document qui énumère les capacités qu'il recherche dans un avenir proche et sollicite des propositions de la part de parties extérieures qui pensent être en mesure de les mettre au point.

« *En matière de désinformation, le Pentagone ne devrait pas combattre le feu par le feu*« , a déclaré Chris Meserole, directeur de l'initiative sur l'intelligence artificielle et les technologies émergentes de la Brookings Institution, à *The Intercept*. « *À l'heure où la propagande numérique se développe dans le monde entier, les États-Unis devraient faire tout ce qui est en leur pouvoir pour renforcer la démocratie en soutenant des notions communes de vérité et de réalité. Les «* deepfakes *» font le contraire. En jetant le doute sur la crédibilité de tous les contenus et de toutes les informations, qu'ils soient réels ou synthétiques, ils finissent par éroder les fondements de la démocratie elle-même*« . Meserole a ajouté : « *Si les «* deepfakes *» doivent être utilisés pour des opérations militaires et de renseignement ciblées, leur utilisation doit faire l'objet d'un examen et d'un contrôle*« .

Le document de lancement, publié pour la première fois par la direction de la science et de la technologie du SOCOM en 2020, établissait une liste de gadgets de nouvelle génération pour le commando des forces spéciales du XXIe siècle, une litanie d'outils futuristes qui aideraient les soldats d'élite du pays à chasser et à tuer plus efficacement leurs cibles à l'aide de lasers, de robots, d'holographes et d'autres équipements sophistiqués.

En octobre dernier, le SOCOM a discrètement publié une version actualisée de sa liste de souhaits, avec une nouvelle section : « *Technologies avancées pour les opérations de soutien à l'information militaire (MISO)*« , un euphémisme du Pentagone pour désigner ses efforts de propagande et de tromperie à l'échelle mondiale.

Le paragraphe ajouté précise que le SOCOM souhaite obtenir des moyens nouveaux et améliorés pour mener des « *opérations d'influence, de manipulation numérique, de perturbation des communications et des campagnes de désinformation au niveau tactique et opérationnel*« . Le SOCOM recherche « *une capacité de nouvelle génération pour collecter des données disparates par le biais de flux d'informations publics et ouverts tels que les médias sociaux, les médias locaux, etc. pour permettre au MISO d'élaborer et de diriger des opérations d'influence*« .

Le SOCOM se bat généralement dans l'ombre, mais sa réputation publique et son empreinte mondiale sont importantes. Composé d'unités d'élite de l'armée de terre, du corps des marines, de la marine et de l'armée de l'air, le SOCOM dirige les opérations militaires les plus sensibles de la nation la plus meurtrière du monde.

Si les forces spéciales américaines sont largement connues pour leurs exploits spectaculaires, comme l'assassinat d'Oussama ben Laden par les Navy SEALs, leur histoire est faite de missions secrètes, de subterfuges, de sabotages et de campagnes de déstabilisation. Les ambitions de désinformation de « *nouvelle génération* » du SOCOM ne sont qu'une partie d'une longue et vaste histoire d'efforts de tromperie de la part de l'armée américaine et des services de renseignement.

Le commandement des opérations spéciales, qui accepte des propositions sur ces capacités jusqu'en 2025, n'a pas répondu à notre demande de commentaire.

Bien que le SOCOM coordonne depuis des années des « *opérations d'influence* » à

l'étranger, ces campagnes de tromperie font l'objet d'un nouvel examen. En décembre, *The Intercept* a rapporté que le SOCOM avait convaincu Twitter, en violation de ses politiques internes, d'autoriser un réseau de comptes fictifs qui diffusaient de fausses nouvelles d'une exactitude douteuse, notamment une affirmation selon laquelle le gouvernement iranien volait les organes de civils afghans. Bien que l'offensive de propagande basée sur Twitter n'ait pas utilisé de « *deep fakes*« , les chercheurs ont constaté que les contractants du Pentagone utilisaient des avatars générés par apprentissage automatique pour conférer aux faux comptes un certain degré de réalisme.

De manière provocante, le document de capacité mis à jour révèle que le SOCOM souhaite renforcer ces efforts de tromperie sur Internet en utilisant des vidéos « *deepfake* » de « *nouvelle génération*« , une méthode de plus en plus efficace pour générer des montages vidéos numériques réalistes à l'aide de l'apprentissage automatique. Les forces spéciales utiliseraient ces séquences truquées pour « *générer des messages et influencer les opérations via des canaux non traditionnels*« , ajoute le document.

Si les « *deepfakes* » sont largement utilisés pour le divertissement et la pornographie, le potentiel d'applications plus terribles est réel. Au début de l'invasion de l'Ukraine par la Russie, un « *deepfake* » de mauvaise qualité montrant le président ukrainien Volodymyr Zelensky ordonnant aux troupes de se rendre a commencé à circuler sur les réseaux sociaux. Les considérations éthiques mises à part, la légalité des *deepfakes* militarisés dans un conflit, qui reste une question ouverte, n'est pas abordée dans le document du SOCOM.

Comme pour les campagnes de « *désinformation* » des gouvernements étrangers, les États-Unis ont passé ces dernières années à mettre en garde contre la menace que représentent les « *deepfakes* » pour la sécurité nationale. L'utilisation de *deepfakes* pour tromper délibérément, avertissent régulièrement les autorités gouvernementales, pourrait avoir un effet profondément déstabilisant sur les populations civiles qui y sont exposées.

Au niveau fédéral, cependant, la conversation a tourné exclusivement autour de la menace que les « *deepfakes* » fabriqués à l'étranger pourraient représenter pour les États-Unis, et non l'inverse. Des documents contractuels publiés précédemment montrent que le SOCOM a recherché des technologies permettant de détecter les campagnes Internet utilisant des *deepfakes*, une tactique qu'il souhaite maintenant mettre en œuvre lui-même.

La section qui suit est peut-être aussi provocante que la mention des « *deepfakes* » : elle indique que le SOCOM souhaite affiner sa propagande offensive en espionnant le public visé à l'aide de ses appareils connectés à l'internet.

Décrit comme une « *capacité de nouvelle génération permettant de « prendre le contrôle » des appareils de l'Internet des objets (IoT) pour collecter [sic] des données et des informations auprès des populations locales afin de permettre la décomposition des messages qui pourraient être populaires et acceptés grâce au tri des données une fois reçues*« , le document indique que la capacité d'écouter les cibles de la propagande « *permettrait au MISO d'élaborer et de promouvoir des messages qui pourraient être plus facilement reçus par la population locale*. » En 2017, *WikiLeaks* a publié des fichiers volés de la CIA qui révélaient une capacité à peu près similaire de piratage des appareils ménagers.

La technologie qui sous-tend les vidéos « *deepfake* » est apparue pour la première fois en 2017, stimulée par la combinaison d'un matériel informatique puissant et bon marché et de percées dans le domaine de l'apprentissage automatique. Les vidéos « *deepfake* » sont

généralement réalisées en envoyant des images d'un individu à un ordinateur et en utilisant l'analyse informatique qui en résulte pour coller un simulacre très réaliste de ce visage sur un autre.

Une fois le logiciel suffisamment entraîné, l'utilisateur peut produire des séquences réalistes d'une cible disant ou faisant pratiquement n'importe quoi. La facilité d'utilisation et la précision croissante de cette technologie font craindre une ère où le public mondial ne pourra plus croire ce qu'il voit de ses propres yeux.

Bien que les principales plateformes sociales comme Facebook aient des règles contre les *deepfakes*, étant donné la nature intrinsèquement fluide et interconnectée d'Internet, les *deepfakes* diffusés par le Pentagone pourraient également risquer de revenir sur le territoire américain.

« *S'il s'agit d'un environnement médiatique non traditionnel, je pourrais imaginer que la forme de manipulation aille assez loin avant d'être arrêtée ou réprimandée par une sorte d'autorité locale*« , a déclaré Max Rizzuto, chercheur sur les deepfakes au Digital Forensic Research Lab de l'Atlantic Council. « *La capacité de nuire à la société est certainement là* ».

L'intérêt du SOCOM pour le déploiement de campagnes de désinformation à base de *deep fakes* fait suite à l'inquiétude internationale suscitée ces dernières années par les vidéos falsifiées et la tromperie numérique des adversaires internationaux. Bien qu'il y ait peu de preuves que les efforts de la Russie pour influencer numériquement l'élection de 2016 aient eu un effet significatif, le Pentagone a exprimé son intérêt pour redoubler ses capacités de propagande numérique, de peur de prendre du retard, le SOCOM jouant un rôle crucial à cet égard.

Lors d'une audition de la commission des forces armées du Sénat en avril 2018, le général Kenneth Tovo, du commandement des opérations spéciales de l'armée, a assuré aux sénateurs réunis que les forces spéciales américaines s'efforçaient de combler le fossé dans la guerre de propagande.

« *Nous avons investi assez lourdement dans nos opérations psychologiques*« , a-t-il déclaré, « *en développant de nouvelles capacités, en particulier pour traiter l'espace numérique, l'analyse des médias sociaux et une variété d'outils différents qui ont été mis sur le terrain par SOCOM et qui nous permettent d'évaluer l'espace des médias sociaux, d'évaluer le domaine cybernétique, de voir l'analyse des tendances, où l'opinion se déplace, et ensuite comment influencer potentiellement cet environnement avec nos propres produits*. »

Alors que la propagande militaire est aussi ancienne que la guerre elle-même, les *deepfakes* ont souvent été discutés comme étant un danger technologique sui generis, dont l'existence constitue une menace civilisationnelle.

Lors d'une audition de la commission sénatoriale du renseignement en 2018 sur la nomination de William Evanina pour diriger le Centre national de contre-espionnage et de sécurité, le sénateur Marco Rubio (R-Fla) a déclaré à propos des *deepfakes* : « *Je pense qu'il s'agit de la prochaine vague d'attaques contre l'Amérique et les démocraties occidentales*. » En réponse, M. Evanina a assuré M. Rubio que les services de renseignement américains s'efforçaient de contrer la menace des « *deepfakes*« .

Le Pentagone serait également à pied d'œuvre pour contrer la menace de

*deepfakes*étrangers. Selon un rapport datant de 2018, la Defense Advanced Research Projects Agency, la division de recherche technologique de l'armée, a dépensé des dizaines de millions de dollars pour mettre au point des méthodes de détection des images truquées. Des efforts similaires sont en cours dans l'ensemble du département de la défense.

En 2019, Rubio et le sénateur Mark Warner (D-Va) ont écrit à 11 entreprises américaines du secteur de l'internet pour leur demander d'élaborer des politiques de détection et de suppression des vidéos truquées. « *Si le public ne peut plus faire confiance aux événements ou aux images enregistrés* », lit-on dans la lettre, « *cela aura un impact corrosif sur notre démocratie* ».

La loi sur l'autorisation de la défense nationale pour l'année fiscale 2021 contenait une directive demandant au Pentagone d'effectuer une « *évaluation de la menace posée par les gouvernements étrangers et les acteurs non étatiques qui créent ou utilisent des médias manipulés par des machines (communément appelés « deep fakes »)*« , y compris « *la manière dont ces médias ont été utilisés ou pourraient être utilisés pour mener une guerre de l'information*« .

Quelques années plus tard, les forces spéciales américaines semblent se préparer à mener le même genre de guerre.

« *C'est une technologie dangereuse*« , a déclaré M. Rizzuto, chercheur à l'Atlantic Council. « *On ne peut pas modérer cette technologie comme on le fait pour d'autres types de contenu sur l'internet*« , a-t-il ajouté. « *Les « deepfakes », en tant que technologie, ont des points communs avec les conversations autour de la non-prolifération nucléaire* ».

Sam Biddle

Article original en anglais : U.S. Special Forces Want to Use Deepfakes for Psy-Ops, The Intercept, le 6 mars 2023.

Traduit par Wayan, relu par Hervé, pour le Saker Francophone

Articles Par : Sam Biddle

media@globalresearch.ca