Réseaux Sociaux: des faux comptes associés à l'armée américaine

Le 22 septembre 2022 par Peter Cronau https://declassifiedaus.org/2022/09/22/declassified-australia-exposes-and-analyses-a-massive-secret-propaganda-operation-being-run-out-of-the-us-that-has-been-buried-by-western-media/

Peter Cronau est un journaliste d'investigation, écrivain et cinéaste primé. Ses documentaires ont été diffusés dans l'émission Four Corners sur *ABC TV* et dans l'émission *Background Briefing* sur *Radio National*. Il est rédacteur et cofondateur de *DECLASSIFIED AUSTRALIA*. Il est co-éditeur du récent livre *A Secret Australia - Revealed by the WikiLeaks Exposés* (*Une Australie secrète - Révélée par les divulgations de WikiLeaks*) Voir tous les messages de Peter Cronau

Ciblant la Russie, la Chine, l'Iran, l'Asie centrale et d'autres pays du Moyen-Orient, l'opération d'information de l'armée américaine visant à diffuser de la propagande est le plus vaste programme d'opérations secrètes d'information pro-occidentales menées sur les médias sociaux qui soit jamais révélé (Image : Stanford Internet Observatory)

«LA PLUS VASTE OPÉRATION SECRÈTE D'INFORMATION PRO-OCCIDENTALE SUR LES MÉDIAS SOCIAUX».

Declassified Australia expose et analyse une vaste opération secrète de propagande menée depuis les États-Unis, qui a été passée sous silence par les médias occidentaux.

On a découvert qu'une opération de propagande en ligne, considérée comme la plus importante au monde pour la promotion des « récits pro-occidentaux », opérait essentiellement depuis les États-Unis et ciblait la Russie, la Chine et l'Iran. «Nous pensons que cette activité représente le cas le plus important d'OI [opération d'information] secrète pro-occidentale sur les médias sociaux qui ait été étudiée et analysée par des chercheurs en accès libre à ce jour», déclarent les chercheurs de l'université de Stanford (https://cyber.fsi.stanford.edu/io/news/sio-aug-22-takedowns) et de *Graphika (https://graphika.com/reports/unheard-voice)*, société de recherche sur Internet.

Les chercheurs ont constaté que la majeure partie de l'opération d'information «provenait probablement des États-Unis». À partir de ce pays, un réseau massif et interconnecté de comptes «robots» automatisés ont été exploités sur Twitter, Facebook et d'autres plateformes de médias sociaux. L'opération secrète visant à influencer les internautes a consisté à utiliser des «techniques de tromperie pour promouvoir des contenus pro-occidentaux» tout en «contrant des pays comme la Russie, la Chine et l'Iran».

«Sur ces comptes la Russie a été fortement critiquée, en particulier pour la mort de civils innocents et autres atrocités commises par ses soldats dans le cadre des «ambitions impériales» du Kremlin après son invasion de l'Ukraine en février de cette année», indique le rapport.

Declassified Australia publie ici une analyse détaillée du remarquable rapport (https://stacks.stanford.edu/file/druid:nj914nx9540/unheard-voice-tt.pdf) de l'Internet Observatory (SIO) de l'université de Stanford et de la société d'analyse de réseaux *Graphika*, publié le 24 août. Ce rapport est d'autant plus surprenant que SIO et *Graphika* ont des liens étroits avec les services de la sécurité nationale américaine et avec les campagnes d'information visant les ennemis désignés par les États-Unis, à savoir la Russie, la Chine et l'Iran.

Le directeur du SIO, Alex Stamos (https://cisac.fsi.stanford.edu/people/alex-stamos), est par exemple membre du Council on Foreign Relations, chercheur invité au Hoover Institute et membre du conseil consultatif du centre

d'excellence en cybersécurité collective de l'OTAN. Il a été responsable de la sécurité chez Facebook, où il a dirigé l'enquête de l'entreprise (https://www.vox.com/2017/10/3/16379724/facebook-alex-stamos-russia-ads-election-donald-trump) concernant la manipulation russe présumée lors de l'élection américaine de 2016.

Alex Stamos (Win McNamee / Getty Images)

Le directeur des enquêtes de *Graphika*, Ben Nimmo, est un chercheur de haut niveau de l'Atlantic Council, il a été consultant pour l'unité de propagande de l'Integrity Initiative britannique, a précédemment travaillé comme attaché de presse pour l'OTAN, et est actuellement chef du renseignement chez Meta (propriétaire de Facebook et Instagram). Il y a produit un rapport (https://public-assets.graphika.com/reports/graphika_report_uk_trade_leaks_updated_12.12.pdf) qui a essayé de lier le leader travailliste Jeremy Corbyn à une opération d'influence russe avant les élections législatives britanniques de 2019.

Ironiquement intitulé « Unheard Voice : Evaluating five years of pro-Western covert influence operations » [Unheard Voice : Évaluation de cinq années d'opérations d'influence secrètes pro-occidentales, NdT], le rapport a été méthodiquement ignoré par la quasi-totalité des médias occidentaux depuis sa publication le mois dernier. Bien que l'opération de propagande ait été menée sur une grande échelle et qu'elle ait été ciblée, les révélations pourtant spectaculaires n'ont suscité qu'une maigre attention, comme cette brève mention (https://www.smh.com.au/world/europe/google-to-inoculate-europeans-by-pre-bunking-ukrainian-refugee-disinformation-20220825-p5bckw.html) dans le *Sydney Morning Herald*.

Une chronique humoristique du *Washington Post* (https://www.washingtonpost.com/politics/2022/08/25/phony-us-friendly-social-media-campaign-prompts-questions/) l'a qualifié de «rapport tape-à-l'œil», affirmant que certains des comptes américains secrets avaient publié des «photos de chats» afin de paraître authentiques. La chronique fait référence aux opérations de cyber-espionnage russes et chinoises pour formuler ses remarques sur le rapport.

Si le rapport a été enterré, cela tient peut-être en partie au fait qu'il a été opportunément éclipsé le jour même de sa publication par un autre rapport du Stanford Internet Observatory intitulé «A Front for Influence: An Analysis of a Pro-Kremlin Network Promoting Narratives on COVID-19 and Ukraine » [Un front pour exercer une influence : Analyse d'un réseau pro-Kremlin faisant la promotion de récits sur le COVID-19 et l'Ukraine, NdT].

L'imposant ensemble de données Twitter-Meta

Les données analysées par Stanford-Graphika ont été publiées après que Twitter et Meta/Facebook eurent supprimé, en

juillet et août 2022, deux séries de faux comptes à caractère similaire pour avoir violé leurs conditions de service. Les ensembles de données semblent couvrir une série de campagnes secrètes sur une période de près de cinq ans plutôt qu'une opération homogène.

Ben Nimmo parcourt le web à la recherche de robots russes. Cela fait de lui une cible. Source New York Times

L'ensemble de données Twitter portait sur 299 566 tweets émis par quelques 146 comptes, alors que l'ensemble de données Meta se concentrait sur 39 profils Facebook et 26 comptes Instagram. Twitter a déclaré que les comptes avaient enfreint ses politiques en matière de «manipulation des plateformes et de spam», tandis que Meta a déclaré que les actifs sur ses plateformes avaient adopté un «comportement non authentique coordonné».

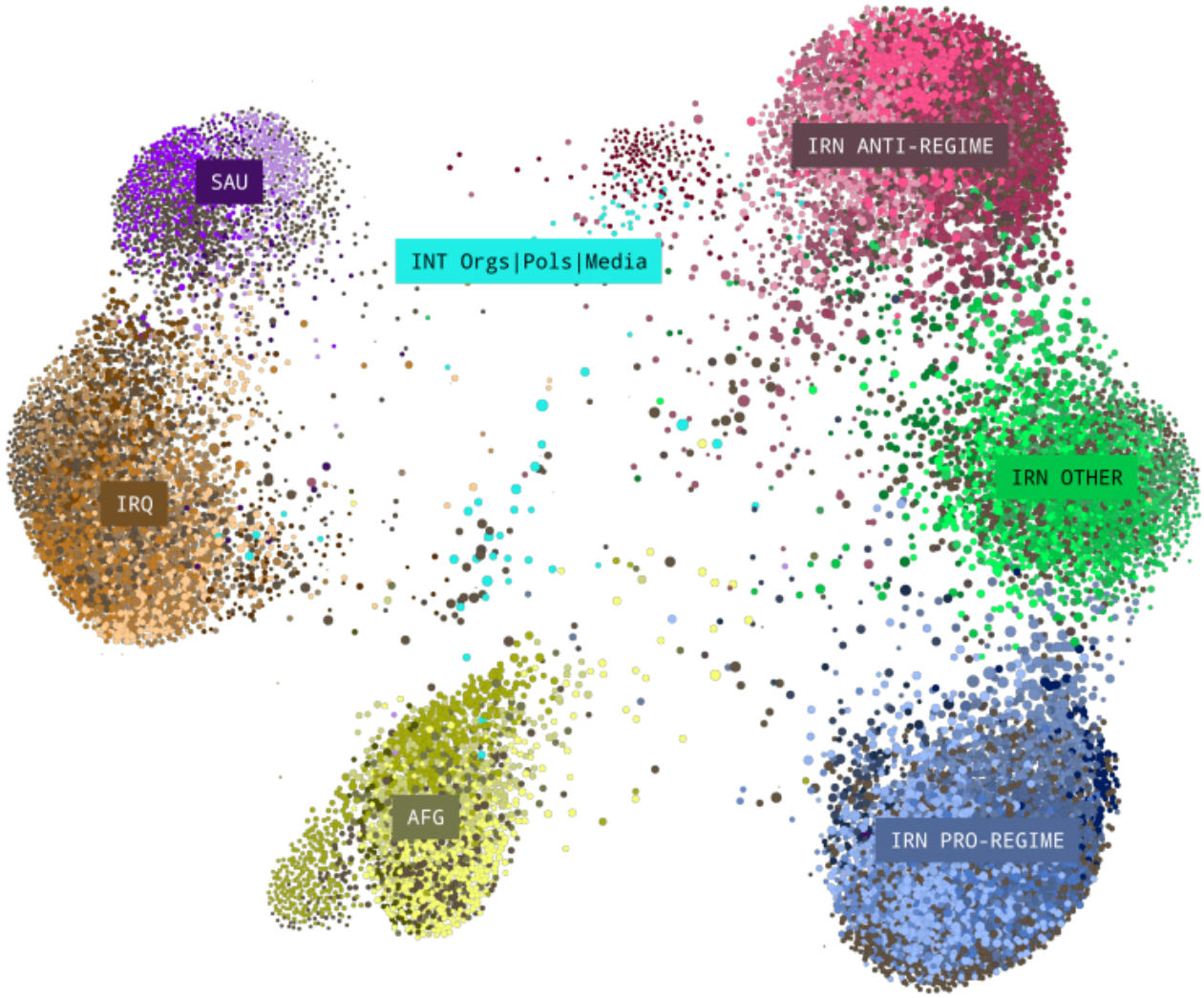


Figure 1: Community network map of covert Twitter asset followers. Color represents major community groupings. Distance reflects network proximity, with accounts appearing close to those they follow and that follow them.

Carte du réseau communautaire des abonnés des faux comptes Twitter des groupes de pression secrets dans les régions d'Iran, Afghanistan, Irak, Arabie saoudite. Les couleurs représentent les principaux groupements communautaires. Les distances reflètent la proximité du réseau, les comptes paraissent proches de ceux qu'ils suivent et de ceux qui les suivent (Image : Stanford Internet Observatory-Graphika)

À un moment donné, le rapport Stanford-Graphika a plutôt eu tendance à minimiser la portée et l'influence des faux comptes: "La grande majorité des [centaines de milliers de] posts et tweets que nous avons examinés n'ont reçu qu'une poignée de likes ou de retweets, et seuls 19% des actifs secrets que nous avons identifiés avaient plus de 1 000 followers".

Bien que cela puisse donner aux détracteurs du rapport du fil à tordre, des centaines de faux comptes comptant des milliers d'abonnés constituent certainement un élément substantiel. En outre, le rapport décrit l'opération comme «le cas le plus important d'OI [opération d'information] secrète pro-occidentale sur les médias sociaux qui ait été étudiée et analysée par des chercheurs travaillant sur des logiciels libres à ce jour».

Les chercheurs n'ont pas identifié les entités américaines qui géraient le programme, mais ils ont noté que: «Les comptes partageaient parfois des articles d'actualité provenant d'organes de presse financés par le gouvernement américain, tels que *Voice of America* et *Radio Free Europe*, et des liens vers des sites Web financés par l'armée américaine».

Parmi les données analysées, deux campagnes de désinformation distinctes ont été identifiées. La première est une campagne de désinformation précédemment exposée, menée par le Pentagone, tandis que la seconde comprend une série d'opérations secrètes d'origine indéterminée.

Dans les fichiers de données, les chercheurs de Stanford-Graphika ont découvert «un lien entre une des campagnes et une opération de communication officielle du gouvernement américain appelée Trans-Regional Web Initiative». La

première preuve de l'existence de ce programme a été apportée en 2012 par le Stimson Center, un groupe de réflexion dont le siège est à Washington - ce document n'est désormais plus en ligne, mais il est archivé ici (https://web.archive.org/web/20220405071328/http:/stimson.org/wp-content/files/file-attachments/Pentagon_as_pitchman_0.pdf).

Ce programme d'influence (https://www.stimson.org/2012/pentagon-pitchman-perception-and-reality-public-diplomacy-0/) "Initiative Web" a été conduit par le Commandement des opérations spéciales (SOCOM) de l'armée américaine au cours des années 2010, et a consisté à déployer des dizaines d'équipes MISO (Military Information Support Operations: opérations de soutien à l'information militaire) dans le cadre d'opérations psychologiques dans le monde entier à la demande des commandants militaires sur le terrain, et des ambassadeurs d'un certain nombre d'ambassades américaines.

Dans le cadre de cette opération de désinformation de plusieurs millions de dollars, le SOCOM avait confié une partie de son travail de développement au groupe Rendon (https://web.archive.org/web/20060612234417/http:/www.rollingstone.com/politics/story/8798997/the_man_who_sold_the_war/), un entrepreneur lié à la CIA et connu pour avoir influencé l'opinion publique et les médias occidentaux avant le début de la guerre en Irak en 2003.

Le SOCOM (https://www.socom.mil/) a notamment élaboré des sites Internet proposant des informations, des reportages culturels, des programmes sportifs et autres destinés à des «publics cibles», tels que Southeast Europe Times et Central Asia Online. Ces sites Web «ont clairement les caractéristiques du journalisme» et cherchent «à présenter les États-Unis et leurs opérations sous un jour positif».

Des réseaux clandestins dévoilés

Les groupes secrets de l'opération d'information (OI) récemment révélés ont été observés de plus près dans le cadre du rapport Stanford-Graphika, qui les a identifiés comme «le cas le plus important d'OI [opération d'information] secrète pro-occidentale sur les médias sociaux» qui ait été étudiée et analysée par des chercheurs travaillant sur des logiciels libres à ce jour.

Les faux comptes clandestins pro-occidentaux identifiés par Twitter et Meta avaient «créé de faux personnages avec des visages GAN (Generative Adversarial Network-computer-generated), s'étaient fait passer pour des médias indépendants, avaient exploité des mèmes et des vidéos de courte durée, avaient tenté de lancer des campagnes de hashtag et lancé des pétitions en ligne».

Un des profils abrités par le cluster Asie centrale utilisait une photo trafiquée (à gauche), de l'actrice Valeria Menendez (à droite) comme photo de profil. L'actif qui a utilisé cette image était répertorié comme le contact de la page VK d'Intergazeta (Image: Stanford Internet Observatory-Graphika)

La cartographie des réseaux de médias sociaux a permis de constater que les comptes Twitter secrets ciblaient des publics du Moyen-Orient, principalement en Iran (45%), en Afghanistan, en Irak et en Asie centrale. L'analyse a également révélé «des groupes de communautés plus modestes dans le réseau, abritant des comptes internationaux mixtes, plus ou moins focalisés sur une variété de personnalités et d'organisations internationales».

Certains de ces comptes secrets ciblaient des régions de Russie et de Chine. «L'opération visait les publics russophones d'Asie centrale et avait pour but de glorifier l'aide américaine à l'Asie centrale et la critique de la Russie, en particulier de sa politique étrangère. Deux actifs se sont concentrés sur la Chine et le traitement des minorités musulmanes chinoises, en particulier les Ouïgours de la province du Xinjiang».

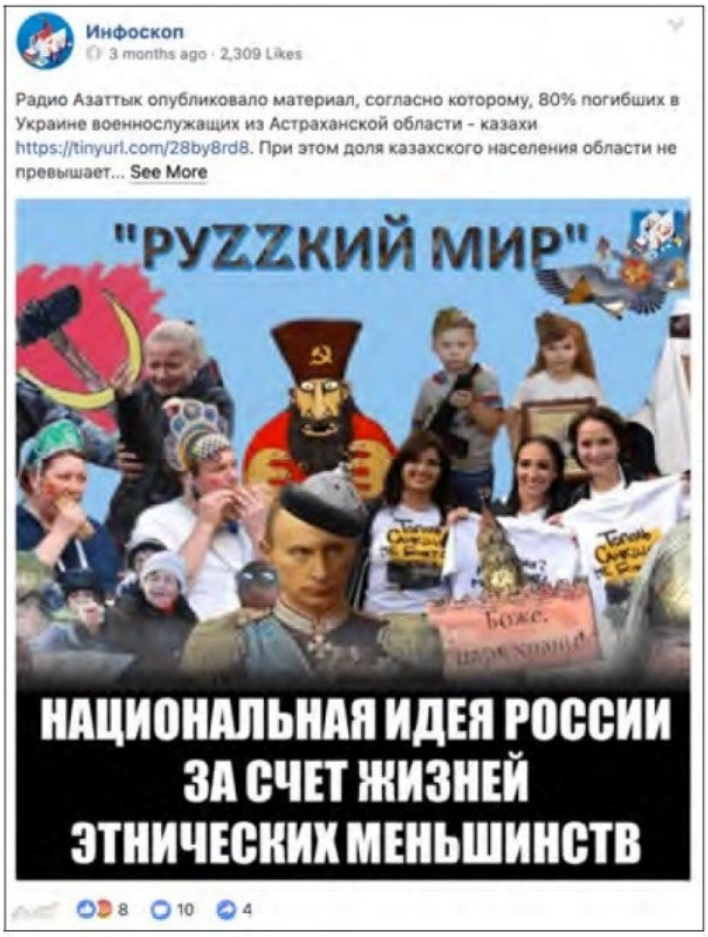
Les chercheurs ont constaté que les groupes de désinformation se focalisaient sur plusieurs sujets pro-occidentaux, à savoir «les efforts diplomatiques et humanitaires des États-Unis dans la région, la prétendue influence néfaste de la Russie, les interventions militaires russes au Moyen-Orient et en Afrique, ainsi que l'"impérialisme" chinois et le traitement des minorités musulmanes».

Le pôle Russie

À partir de février, l'Ukraine est devenue le centre d'intérêt d'une grande partie de l'opération secrète sur Twitter. Les chercheurs ont constaté que «les ressources qui publiaient auparavant des informations sur les activités militaires russes au Moyen-Orient et en Afrique se sont tournées vers la guerre en Ukraine, présentant le conflit comme une menace pour les populations d'Asie centrale».

«Peu après le début de l'invasion en février, certains comptes ont largement relayé les manifestations pro-ukrainiennes dans les pays d'Asie centrale. Des posts ultérieurs ont fait état de preuves d'atrocités commises par les troupes russes et du blocus instauré par la Russie concernant les exportations de céréales ukrainiennes. L'opération secrète, faisant état des ambitions «impériales» de la Russie, a présenté les États-Unis comme «le principal garant de la souveraineté de l'Asie centrale face à la Russie».

«D'autres publications dénonçaient le recours de la Russie à la propagande pour diffuser des récits anti-Occidentaux et pro-russes en Asie centrale, et décrivaient la Russie comme une puissance maléfique s'efforçant de saper les démocraties indépendantes». L'opération secrète a permis de créer des «fausses personnalités» liées à des «médias fictifs», sous prétexte de diffuser des informations sur les événements en Asie centrale. Plusieurs de ces sites et pages ont attiré jusqu'à 6 000 abonnés.



Publications laissant entendre que la Russie a l'intention d'utiliser des minorités ethniques pour combattre en Ukraine (à gauche), et les conséquences funestes de la conscription de migrants d'Asie centrale dans l'armée russe (à droite). (Image : Stanford Internet Observatory-Graphika)

Les données concernant la transparence de Facebook ont montré que les administrateurs de quatre des fausses pages se trouvaient en France, mais l'analyse de Meta a révélé qu'ils étaient en fait «originaires des États-Unis». Plusieurs pages postaient des photos de Paris et de ses monuments pour tenter de masquer leur réelle origine qui était américaine.

Plusieurs sites de fausses «informations», tels qu'Intergazeta et Vostochnaya Pravda, traduisaient en russe des contenus provenant des sites Web de la branche russe de la BBC, des ambassades américaines en Asie centrale et de Radio Free Europe qui est financée par les États-Unis. Par ailleurs, ils ont souvent récupéré du contenu auprès de médias directement financés par le US Central Command (https://www.centcom.mil/), notamment *Caravanserai ()*.

Au moins quatre de ces médias fictifs «ont semble-t-il tenté de lancer des campagnes de hashtag liées à la guerre en Ukraine». Un site publiant des informations sur l'invasion russe en Ukraine a utilisé le hashtag pas vraiment subtil traduit par #TodayUkraineTomorrowCentralAsia. Selon les analyses d'audience effectuées dans le cadre du rapport, ces tentatives n'ont pas eu beaucoup de succès.

Le pôle Chine

Les chercheurs ont constaté qu'un petit groupe d'actifs du groupe Asie centrale se concentrait presque exclusivement sur la Chine. «Ces comptes - un faux profil et un média fictif - se concentraient tout particulièrement sur le génocide des Ouïghours et des minorités musulmanes dans les camps de «rééducation» du Xinjiang».

Les messages faisaient état «d'allégations de trafic d'organes, de travail forcé, de crimes sexuels contre les femmes musulmanes et de disparitions suspectes de musulmans ayant une appartenance ethnique au Xinjiang». D'autres actifs du groupe ont également posté des messages concernant la Chine, affirmant que «l'autoritarisme et l'impérialisme financier chinois menaçaient l'Asie centrale et d'autres régions du monde».

Posts au sujet de supposés prélèvements d'organes effectués sur des musulmans au Xinjiang (à gauche), et concernant la Chine accusée d'être le principal commanditaire de la guerre de la Russie contre l'Ukraine (à droite) (Image : Stanford Internet Observatory-Graphika)

Ces profils clandestins sur les médias sociaux «font fréquemment référence à la coopération de la Chine avec la Russie, notamment sur les questions militaires, et affirment que Pékin devrait être tenu pour responsable de l'invasion de l'Ukraine par la Russie, car le PCC a secrètement fourni des armes au Kremlin».

Ce faux narratif selon lequel la Chine fournirait à la Russie des armes pour la guerre en Ukraine a également été diffusée en Occident, mais il a été rapidement démenti, et aujourd'hui, même l'armée ukrainienne (https://mil.in.ua/en/news/the-us-sees-no-signs-of-china-supplying-russia-with-weapons/) a admis que cette histoire était fausse.

Le pôle Iran

Les faux profils appartenant au groupe Iran «prétendent régulièrement être des citoyens iraniens et souvent des femmes [dont] les professions indiquées sont «professeur» et «militant politique» ». Certains des faux médias en langue persane ont fait preuve d'une certaine audace. Le slogan de la chaîne YouTube *Fahim News* est «Des nouvelles et des informations exactes». *Dariche News* prétend fournir des «informations non censurées et impartiales» et déclare être «un site web indépendant... non affilié à un groupe ou une organisation».

Le contenu destiné aux faux médias iraniens provient de sites en langue perse financés par les États-Unis, mais aussi de la chaîne de télévision britannique *Iran International*, qui serait financée par un homme d'affaires ayant des liens avec le prince héritier saoudien (https://www.theguardian.com/world/2018/oct/31/concern-over-uk-based-iranian-tv-channels-links-to-saudi-arabia) Mohammed bin Salman.

Le 18 août 2022, un message du faux média *Fahim News* affirmait que les médias sociaux sont le seul moyen pour les Iraniens d'accéder au monde libre et qu'ils sont le principal ennemi de la propagande du régime iranien. «C'est pourquoi le régime déploie tous ses efforts pour censurer et filtrer l'Internet».

Il est certain que ceux qui colportent la désinformation aiment jouer un double jeu. Les profils appartenant au cluster Iran présentaient certaines caractéristiques de spam, probablement destinées à générer une vaste audience en ligne. De nombreux comptes «publiaient des contenus fictifs non politiques», notamment de la poésie iranienne, des photos de cuisine persane et même d'adorables photos de chats.

Cette image a été tweetée par un pseudo-actif le 24 février 2022, et indique «Liberté d'expression en Iran». Le texte accompagnant le tweet a utilisé deux hashtags persans, l'un protestant contre un projet de loi sur le contrôle de l'Internet, et l'autre disant «Non à la République islamique» (Image : Stanford Internet Observatory-Graphika)

«Nous avons observé dans le groupe Iran, de nombreux cas de comptes partageant du contenu provenant de sources liées à l'armée américaine». Sans doute fruit d'une maladresse, un compte Twitter qui se présentait comme étant celui d' «un Iranien vivant à Cambridge» a posté des liens vers *Almashareq* et *Diyaruna*, deux sites d'information en langue

perse financés par le Commandement central américain. Le cluster Iran a également mis l'accent sur un point qui fâche le gouvernement iranien - les droits des femmes. «Les posts soulignaient également que peu de choses ont changé pour les femmes en Iran au fil du temps. De nombreux posts mettaient en avant les manifestations nationales visant à dénoncer les exigences vestimentaires de port du hijab».

Le pôle Afghanistan

On a aussi découvert un nombre plus restreint d'actifs afghans qui utilisaient des techniques similaires aux autres groupes, tels que des photos de profil créées par l'IA, des sites de fausses nouvelles et des informations provenant de sources américaines. Les sites «proposaient systématiquement des narratifs critiquant l'Iran et ses pratiques». Parfois, ces récits étaient accompagnés d'affirmations provocatrices et d'articles provenant du site Web *afghanistan.asia-news.com*, un site affilié à l'armée américaine».

Le rapport cite un de ces exemples de provocation: «Un tweet du 11 mars 2022 affirmait que des parents de réfugiés afghans décédés avaient signalé que des corps avaient été renvoyés d'Iran avec des organes manquants». L'article comprend des interviews d'un prétendu officiel afghan et d'une infirmière afghane formulant les mêmes affirmations non vérifiées.

Depuis la chute de l'Afghanistan tombé aux mains des talibans en août 2021, les faux sites ont «mis en lumière les manifestations des femmes contre les autorités talibanes et critiqué le nouveau gouvernement afghan pour la façon dont étaient traités les femmes et les journalistes».

Le pôle Moyen-Orient

Le groupe Moyen-Orient a utilisé ses ressources secrètes pour se concentrer sur des questions liées principalement à l'Irak, la Syrie, le Liban et le Yémen. Ce groupe a «principalement promu des récits visant à saper l'influence de l'Iran dans la région». Pour ce faire, il a diffusé des allégations et des récits enflammés ayant pour but d'influencer le public.

Plusieurs faux comptes Twitter «se sont fait passer pour des militants irakiens afin de pouvoir accuser l'Iran de menacer la sécurité hydrique en Irak et d'inonder le pays de méthamphétamine». «D'autres actifs ont souligné que les mines terrestres placées par les Houthis tuent des civils, et ont soutenu les allégations selon lesquelles l'invasion de l'Ukraine par la Russie entraînera une crise alimentaire mondiale».

De nombreux profils ont publié un contenu similaire, au même moment, qui était clairement partagé et concerté. Les opérateurs du cluster du Moyen-Orient font également preuve d'un certain manque de rigueur en matière de sécurité opérationnelle.

Une page Twitter supposée être celle d'un Irakien du nom de «Discoverer» et utilisant une fausse photo de profil générée par l'IA, publiait principalement des messages concernant les malversations du gouvernement iranien. Toutefois, les versions archivées du compte Twitter montrent qu'avant mai 2021, il utilisait une photo de profil différente, identifiée comme un «compte appartenant au Commandement central des États-Unis», et se trouvait en «Floride, États-Unis».

Photos de profil générées par ordinateur utilisées par les faux comptes Twitter du groupe du Moyen-Orient. (Image : Stanford Internet Observatory-Graphika)

Soit dit en passant, la Floride est aussi le lieu où se trouve le quartier général du Commandement central américain ou CENTCOM, sur la base aérienne MacDill à Tampa, en Floride. Et comme par hasard, la zone de responsabilité du CENTCOM couvre le Moyen-Orient, l'Asie centrale et certaines parties de l'Asie du Sud, soit la même région du globe que celle couverte par les opérations d'information dont il est question ici.

Ainsi, le CENTACOM déclare utiliser des campagnes d'opérations d'information (https://www.centcom.mil/ABOUT-US/SASC-POSTURE-STATEMENT-2017/) (OI) qui «comprennent des messages de contre-propagande... sur Internet et les médias sociaux». Ces campagnes d'OI servent de «multiplicateur de puissance dans l'espace d'information... pour contrer les activités déstabilisatrices commanditées par des États dans la zone de responsabilité du CENTCOM».

Établir la responsabilité de l'«opération d'information»

Déterminer avec une certitude absolue quelle est l'origine de ces opérations d'influence sans précédent relatées ici n'est, selon les rédacteurs du rapport, pas possible. Toutefois, si l'on utilise un critère de preuve utilisé par *Graphika*, un des chercheurs de ce rapport, pour inculper la Russie dans une opération précédente de campagne d'influence, il est surprenant qu'ils n'aient pas pu parvenir à une conclusion plus rigoureuse.

Un tweet du personnage Twitter « Discoverer », qui dans un profil précédent s'était identifié comme vivant en Floride, aux États-Unis, critiquait les actions des mandataires iraniens en Irak et faisait l'éloge des efforts humanitaires du gouvernement américain (Image : Stanford Internet Observatory-Graphika)

En décrivant une fuite de documents commerciaux qui menaçaient de profiter au Parti travailliste britannique lors des élections générales britanniques de 2019, Ben Nimmo, de *Graphika*, a analysé celles-ci et a ensuite noté qu'il «ne peut pas établir la provenance de l'opération», cependant le rapport a courageusement déclaré que :

- «les fuites étaient diffusées d'une manière similaire à l'opération russe Secondary Infektion» [gigantesque campagne de désinformation menée par la Russie pour promouvoir les intérêts nationaux du pays, NdT].
- «les fuites étaient amplifiées en ligne d'une manière qui ressemble beaucoup à une opération d'information russe connue».
- «Les similitudes sont trop importantes pour être une simple coïncidence».
- «Le compte ... a fait des erreurs spécifiques qui étaient caractéristiques de Secondary Infektion».
- «Les tweets ... ressemblaient aux efforts d'amplification antérieurs de Secondary Infektion».

Le rapport (https://graphika.com/reports/uk-trade-leaks) de *Graphika* était intitulé sans ambages: «UK Trade Leaks: Des opérateurs désireux de cacher leur identité ont diffusé des documents commerciaux britanniques et américains ayant fait l'objet de fuites, de manière similaire à l'opération russe Secondary Infektion dévoilée en juin 2019». Ce qui allait se passer ensuite était évident.

Comme on pouvait s'y attendre, les médias grand public ont repris le rapport, le qualifiant systématiquement d'opération de désinformation russe, avec des titres tels que «La Russie est impliquée (https://www.theguardian.com/uk-news/2019/dec/07/russia-involved-in-leak-of-papers-saying-nhs-is-for-sale-says-reddit) dans la fuite de documents» pour le *Guardian*, «Les documents divulgués cités par Corbyn sont liés à un groupe russe (https://news.sky.com/story/leaked-documents-cited-by-corbyn-tied-to-russian-group-reddit-11880096)» pour *SkyNews* et «Les Russes ont tenté d'interférer (https://www.telegraph.co.uk/politics/2020/07/16/russians-tried-interfere-election-promoting-leaked-trade-documents/) dans les élections en faisant la promotion des documents commerciaux divulgués par Jeremy Corbyn» pour le *Telegraph*.

Les implications d'une telle condamnation ont contribué à couler (https://www.abc.net.au/news/2019-12-13/labour-party-begins-to-turn-on-jeremy-corbyn/11796754) la campagne électorale du leader travailliste Jeremy Corbyn.

Le rapport *Stanford-Graphika* «Unheard Voice» permet de tirer certaines conclusions avec un degré élevé de certitude. En fait, celui-ci semble dépasser celui du rapport «UK Trade Leaks» de *Graphika*.

L'objectif, le ciblage, les narratifs, les techniques employées, les sources et même certaines des métadonnées laissées dans leur sillage montrent clairement qui sont ceux qui ont initié des opérations d'information secrètes identifiées dans le rapport «Unheard Voice» de *Stanford-Graphika*. Les prestataires qui fournissent les ensembles de données sur lesquels est basée cette étude ont exprimé leur point de vue - Twitter déclare que les «pays d'origine présumés» de leurs données sont les États-Unis et le Royaume-Uni, et pour Meta, «le pays d'origine» est en fait les États-Unis.

On peut affirmer avec certitude que les opérations d'information, rapportées dans le rapport *Stanford-Graphika* et décrites ici par *Declassified Australia*, sont menées par des groupes ou des individus affiliés à des entités militaires américaines et qu'elles visent à promouvoir des objectifs militaires et impériaux des États-Unis dans les pays ciblés. Ces derniers sont tous considérés comme des ennemis déclarés des États-Unis et il est prouvé que les méthodes et techniques exposées dans le rapport ont été utilisées par les unités de propagande de l'armée américaine et, dans certains cas, les liens sont directs. Une grande partie de leurs sources d'informations proviennent de sites de médias financés par les États-Unis, d'ambassades américaines et d'unités militaires américaines et, enfin, les métadonnées pointent vers l'armée américaine.

Deux sources privilégiées ont depuis lors parlé sous couvert d'anonymat (https://www.washingtonpost.com/national-security/2022/09/19/pentagon-psychological-operations-facebook-twitter/) de cette «opération d'information secrète pro-occidentale la plus vaste sur les médias sociaux», déclarant au *Washington Post* que «le Commandement central des États-Unis fait partie de ceux dont les activités font l'objet d'un examen minutieux».

À ce stade, rien ne semble contredire la conclusion selon laquelle cette opération d'information sans précédent est une vaste opération secrète de propagande militaire américaine.

Peter Cronau