Quand les gouvernements infiltrent internet

Le 24 février 2014 par Glenn Greenwald https://theintercept.com/document/2014/02/24/art-deception-training-new-generation-online-covert-operations/

La psychologie, un nouveau type de SIGDEV

SIGDEV: développe des outils et des méthodes pour vous aider à trouver le trafic que vous désirez

L'une des nombreuses histoires brûlantes qui reste à raconter à partir des archives Snowden est la façon dont les agences de renseignement occidentales tentent de manipuler et de contrôler les échanges en ligne en recourant à des stratégies extrêmes de duperie et de destruction de réputation. Il est temps de raconter un pan de cette histoire, accompagnée des documents pertinents.

Au cours des dernières semaines, j'ai collaboré avec *NBC News* pour publier une série d'articles sur les tactiques de «coups bas» (https://www.nbcnews.com/news/investigations/snowden-docs-british-spies-used-sex-dirty-tricks-n23091) utilisées par l'unité précédemment secrète du GCHQ [le service gouvernemental du Royaume-Uni responsable du renseignement d'origine électromagnétique et de la sécurité des systèmes d'information, NdT], le JTRIG (Joint Threat Research Intelligence Group).

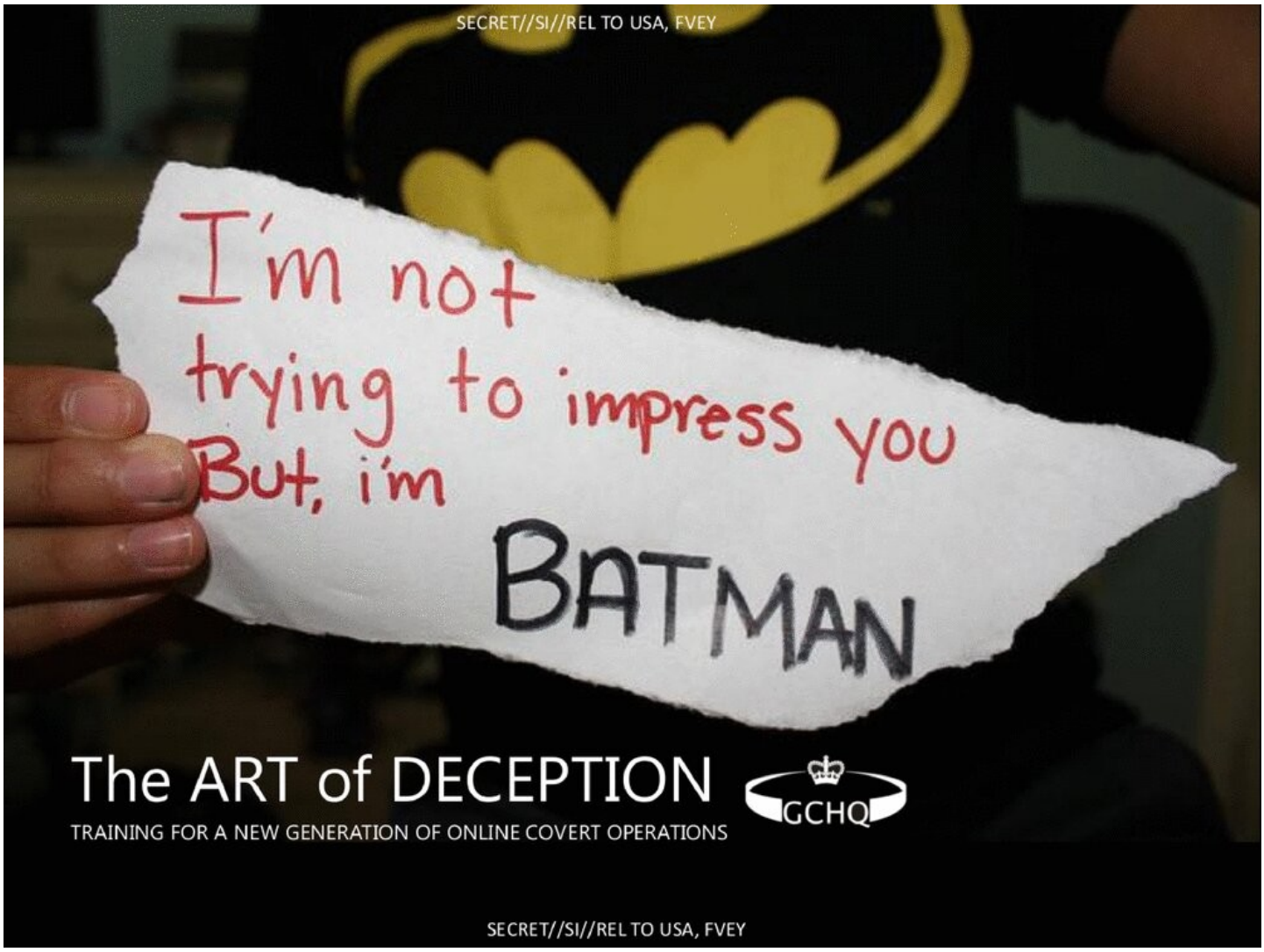
Ces articles se fondaient sur quatre documents classifiés du GCHQ présentés à la NSA et aux trois autres partenaires de l'alliance anglophone «Five Eyes» (https://www.theatlantic.com/politics/archive/2013/06/is-the-five-eyes-alliance-conspiring-to-spy-on-you/277190/). Aujourd'hui, à *The Intercept,* nous publions un autre nouveau document du JTRIG, dans son intégralité, il est intitulé «The Art of Deception: Training for Online Covert Operations». (https://theintercept.com/document/2014/02/24/art-deception-training-new-generation-online-covert-operations/). [L'art de la désinformation : formation pour des opérations secrètes en ligne, NdT]

En publiant ces histoires une par une, notre reportage de la *NBC* a mis en lumière certaines des révélations majeures et confidentielles: la surveillance de *YouTube* et de *Blogger*, le ciblage des *Anonymous* au moyen de ces mêmes attaques DDoS [attaque par déni de service distribué (**DDoS**) est une tentative malveillante de perturber le trafic normal d'un serveur, service ou réseau ciblé, NdT] qu'ils accusent les « hacktivistes » d'utiliser, l'utilisation de « pièges à miel » (attirer les gens dans des situations compromettantes en utilisant le sexe) et de virus destructeurs.

Mais, ici, je veux me concentrer et développer le point essentiel révélé par tous ces documents: à savoir que ces agences tentent de contrôler, d'infiltrer, de manipuler et de déformer les échanges en ligne et, ce faisant, compromettent l'intégrité de l'internet lui-même.

Parmi les principaux objectifs auto-identifiés de la JTRIG figurent deux tactiques : (1) injecter toutes sortes de faux documents sur Internet afin de détruire la réputation des cibles ; et (2) utiliser les sciences sociales et d'autres techniques pour manipuler le discours et l'activisme en ligne afin de générer les résultats qu'elle juge souhaitables.

Pour se rendre compte de l'extrémisme de ces programmes, il suffit de considérer les tactiques qu'ils se targuent d'utiliser pour parvenir à leurs fins : les « opérations sous faux drapeau » (publication de documents sur Internet en les attribuant faussement à quelqu'un d'autre), les faux billets de blog de victimes (en prétendant être une victime de l'individu dont ils veulent détruire la réputation) et la publication « d'informations négatives » sur divers forums.



L'art de la désinformation: formation pour des opérations secrètes en ligne

Voici une liste illustrative de tactiques tirée du dernier document du GCHQ que nous publions aujourd'hui :

MANUEL DE DISRUPTION

- opération d'infiltration
- opération de fraude
- opération de décor
- opération sous fausse bannière
- fausse opération de sauvetage
- opération de déstabilisation
- opération d'infiltration

D'autres tactiques visant des individus sont énumérées ici, sous le titre révélateur « discréditer une cible » :

- mettre en place une souricière
- changer les photos sur les profils de réseaux sociaux
- écrire un blog en prétendant être une de leurs victimes
- envoyer des mails, sms etc à leur famille, voisins, collègues etc.

Ensuite, il y a les tactiques utilisées pour détruire les entreprises que l'agence cible :

- faire fuiter des informations confidentielles à d'autres compagnies/à la presse via des blogs
- poster des appréciations négatives sur les forums appropriés
- mettre fin à des transactions/ruiner des relations d'affaires

Le GCHQ décrit l'objectif de la JTRIG en termes très clairs: «Utiliser des techniques en ligne pour faire bouger les choses dans le monde réel ou cybernétique», y compris les «opérations d'information (influence ou perturbation)».

La proposition qui fait froid dans le dos d'un confident d'Obama (Source Salon Independent)

- utiliser des techniques internet pour faire en sorte que quelque chose se produise dans le monde réel ou le monde virtuel

- 2 catégories au sens large
  - opérations d'information (influence ou déstabilisation)
  - incident informatique

- connu au sein du GCHQ sous le nom de Action Secrète en Ligne

- les 4 D: dénier / déranger / détériorer / décevoir

Il est important de noter que les «cibles» de cette duperie et de cette destruction de réputation vont bien au-delà de la liste habituelle des espions: il s'agit des nations hostiles et leurs dirigeants, des agences militaires et des services de renseignement.

En fait, nombre de ces techniques sont abordées dans le contexte de leur utilisation plutôt que dans celui de la «répression traditionnelle» contre des personnes soupçonnées (mais non inculpées ou condamnées) de crimes ordinaires ou, plus simplement encore, «d'hacktivisme», c'est-à-dire de ceux qui recourent à des actions de contestation en ligne à des fins politiques.

La page titre de l'un de ces documents témoigne de la conscience qu'a l'agence elle-même de «repousser les limites» en utilisant des techniques «cyber-offensives» contre des personnes qui n'ont rien à voir avec le terrorisme ou les menaces pour la sécurité nationale, et qui, en fait, font intervenir de manière centrale des agents chargés de l'application de la loi qui enquêtent sur des crimes ordinaires.

Session de Cyber-offensive: Repousser les limites et agir contre l'Hacktivisme

Quelle que soit votre opinion sur les *Anonymous*, que selon vous ils soient des «hacktivistes» ou de vulgaires délinquants, il n'est pas difficile de comprendre à quel point il est dangereux que des agences gouvernementales occultes puissent cibler les personnes de leur choix – des gens qui n'ont jamais été accusés, et encore moins condamnés, pour

un quelconque délit – avec ce genre de tactiques en ligne, basées sur la duperie, pour détruire et compromettre leur réputation.

Barack Obama a ordonné la révision de la surveillance de la NSA à la suite des révélations d'Edward Snowden (Rex Features)

Comme Jay Leiderman l'a démontré dans le *Guardian (https://www.theguardian.com/commentisfree/2013/jan/22/paypal-wikileaks-protesters-ddos-free-speech)* dans le cas de la répression des hacktivistes de *Paypal 14*, il y a tout lieu de penser que les tactiques de «déni de service» utilisées par les hacktivistes entraînent (tout au plus) des dommages insignifiants, nettement inférieurs aux tactiques de cyberguerre privilégiées par les États-Unis et le Royaume-Uni (https://www.theguardian.com/commentisfree/2012/nov/23/anonymous-trial-wikileaks-internet-freedom), et s'apparentent bien davantage au type de contestation politique protégé par le Premier amendement.

Le point le plus important est que, bien au-delà de la question des hacktivistes, ces agences de surveillance se sont arrogé le pouvoir de délibérément nuire à la réputation des gens et de compromettre leur activité politique en ligne, même s'ils n'ont été accusés d'aucun crime et si leurs actions ne présentent aucun lien plausible avec le terrorisme ni même avec des menaces pour la sécurité nationale.

Comme me l'a dit Gabriella Coleman, spécialiste des *Anonymous* à l'Université McGill, «cibler les *Anonymous* et les hacktivistes revient à cibler des citoyens qui expriment leurs convictions politiques, ce qui a pour effet d'étouffer toute dissidence légitime». Faisant référence à l'étude qu'elle a publiée, la professeure Coleman a contesté avec véhémence l'affirmation selon laquelle «leurs actions ont un caractère terroriste/violent».

Depuis longtemps, on spécule sur les projets gouvernementaux visant à surveiller et à influencer les communications sur Internet, et à infiltrer subrepticement les groupes en ligne afin de semer la discorde et de diffuser de fausses informations.

Cass Sunstein, professeur de droit à Harvard, proche conseiller d'Obama et ancien chef de l'Office of Information and Regulatory Affairs de la Maison Blanche, a rédigé en 2008 un document controversé (https://www.salon.com/2010/01/15/sunstein_2/) dans lequel il proposait que le gouvernement américain emploie des équipes d'agents secrets et de pseudo-défenseurs «indépendants» pour «infiltrer de manière cognitive» des groupes en ligne et des sites web, de même que d'autres groupes d'activistes.

Sunstein a également proposé d'envoyer des agents secrets dans des « salons de discussion [ou clavardoir, lieu de rencontre virtuel, accessible à partir d'un site, NdT], des réseaux sociaux en ligne ou même des groupes dans l'espace réel » susceptibles de diffuser ce qu'il considère être des «théories du complot» mensongères et préjudiciables au gouvernement.

Comble de l'ironie, ce même Sunstein a récemment été nommé par Obama pour faire partie de la commission d'examen de la NSA créée par la Maison Blanche, qui – tout en contestant les principales affirmations de la NSA – a proposé de nombreuses réformes cosmétiques (https://www.theguardian.com/world/2013/dec/13/nsa-review-to-leave-spying-programs-largely-unchanged-reports-say) relatives aux pouvoirs de l'agence (dont la plupart ont été ignorées par le président qui en avait désigné les membres).

Le GCHQ craint un recours en justice au titre de la loi sur les droits humains si les preuves de ses méthodes de surveillance sont déclarées recevables par les tribunaux (Barry Batchelor/PA)

Mais ces documents du GCHQ sont les premiers à prouver qu'un grand gouvernement occidental utilise certaines des techniques les plus controversées pour diffuser de la duperie en ligne et nuire à la réputation de ses cibles. Dans le cadre de ces tactiques, l'État diffuse délibérément des mensonges sur Internet au sujet des individus qu'il cible, notamment en recourant à ce que le GCHQ lui-même appelle des «opérations sous faux drapeau» et en envoyant des courriels aux familles et aux amis des personnes concernées.

Qui pourrait faire confiance à un gouvernement qui exercerait ces pouvoirs, sans parler du fait qu'il le ferait en toute opacité, sans aucun contrôle et en dehors de tout cadre légal? Et puis il y a aussi l'utilisation de la psychologie et d'autres sciences sociales non seulement pour comprendre, mais aussi pour façonner et contrôler le déroulement du militantisme et des échanges en ligne.

Le nouveau document que nous publions aujourd'hui souligne le travail de la «Human Science Operations Cell» [Cellule des opérations de sciences humaines, NdT] du GCHQ, qui a pour mission le «renseignement humain en ligne» et «les stratégies d'influence et de déstabilisation».

Sous le titre «Online Covert Action» [Action secrète en ligne, NdT], le document détaille un ensemble des moyens utilisés pour mener des «opérations en ligne liées à l'influence et à l'information» ainsi que des «désorganisations et des attaques de réseaux informatiques», tout en expliquant très en détail la façon dont les êtres humains sont susceptibles d'être manipulés à l'aide de «leaders», de «confiance», d' «obéissance» et de «soumission».

Les documents exposent des théories sur la façon dont les êtres humains interagissent, en particulier en ligne, puis tentent ensuite d'identifier les moyens permettant de peser sur les résultats - ou de les «manipuler»

Les stratagèmes de la tromperie

Comment se servir, en les analysant et en les détournant de:

- l'attention

- la perception
- la fabrication de sens
- la sensation
- le comportement

Comment identifier et exploiter les points de fracture

Quels sont les outils à utiliser :

- travailler en miroir
  - langage du corps
  - indices fournis par le corps
  - expressions
  - mouvements oculaires
  - émotions

- Adaptation
  - adapter son langage, ses façons d'être pour amender la communication
  - utiliser les convergences dans une discussion
  - utiliser l'empathie et se servir d'autres traits de personnalité
  - attention à la sur-adaptation qui finirait par se traduire par de la condescendance

- Mimétisme
  - adopter des traits sociaux spécifiques en imitant l'autre participant

Nous avons envoyé de nombreuses questions au GCHQ, notamment :

(1) Le GCHQ se livre-t-il à des «opérations sous fausse bannière», dans le cadre desquelles des documents sont publiés sur Internet et faussement attribués à quelqu'un d'autre?

(2) Le GCHQ s'efforce-t-il d'influencer ou de manipuler le discours politique en ligne?

(3) Le mandat du GCHQ inclut-il le ciblage de criminels ordinaires (tels que les opérateurs de *boiler room* [Dans le monde des affaires, le terme *boiler room* (centre d'appel) désigne un centre d'appels sortants vendant des investissements douteux par téléphone. Les vendeurs utilisent des tactiques de vente déloyales et malhonnêtes, terme souvent utilisé de façon péjorative pour désigner des tactiques de vente sous pression et, parfois, de mauvaises conditions de travail, NdT]), ou uniquement celui des menaces étrangères?

Comme à leur habitude, ils ont fait fi de ces questions et ont préféré envoyer un texte passe partout vague et dénué de réponse: «Notre politique traditionnelle est de ne pas faire de commentaires en matière de renseignement. En outre, toutes les activités du GCHQ sont menées conformément à des règles juridiques et politiques strictes qui garantissent que nos activités sont dûment autorisées, nécessaires et proportionnées, et qu'elles font l'objet d'une surveillance rigoureuse, notamment de la part du secrétaire d'État, des commissaires aux services d'interception et de renseignement et du comité parlementaire sur le renseignement et la sécurité. Tous nos processus opérationnels vont rigoureusement dans ce sens».

Le fait que ces agences refusent de «commenter les questions de renseignement» – c'est à dire de parler de tout ce qu'elles font – explique précisément pourquoi la dénonciation est si urgente, le journalisme qui y contribue si clairement dans l'intérêt du public et les attaques de plus en plus délirantes de ces agences si faciles à comprendre (https://www.theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance-secret-snowden).

Les affirmations selon lesquelles les agences gouvernementales infiltrent les communautés en ligne et s'engagent dans des « opérations sous faux drapeau » pour discréditer leurs cibles sont souvent écartées, qualifiées de théories du complot, mais ces documents ne laissent aucun doute quant au fait que c'est précisément ce qu'elles font.

Quoi qu'il en soit, un gouvernement ne devrait pas être en mesure de recourir à ces stratégies : comment justifier que des agences gouvernementales ciblent des individus – qui n'ont été accusés d'aucun crime – pour détruire leur réputation, infiltrer des groupes politiques en ligne et développer des techniques pour manipuler les échanges en ligne ?

Mais il est particulièrement indéfendable d'autoriser ces agissements sans que le public en soit informé et sans que quiconque ait à rendre des comptes.

We want to build Cyber *Magicians*.

SECRET//SI//REL TO USA, FVEY

Nous voulons former des cyber magiciens (Source he Intercept) https://theintercept.com/2014/02/24/jtrig-manipulation/