Lettre n°51-Juin 2016-disponible sur omc.ceis.eu

« This is about developing our capabilities and ability to partly protect NATO cyber networks but also to help and assist nations in defending their cyber networks. […] Since it's very hard to imagine a military conflict today without a cyber dimension, this is important, related to almost all possible conflicts we can foresee in the future. » Jens Stoltenberg, Secrétaire général de l'OTAN[1], au sujet de la définition du cyberespace en tant que domaine opérationnel à part entière de l'organisation.

Table des matières

1 http://www.infosecurity-magazine.com/news/cyberspace-is-new-domain-for-war/

RETOUR SUR LA DEUXIÈME PHASE DE L'OPÉRATION #OPICARUS

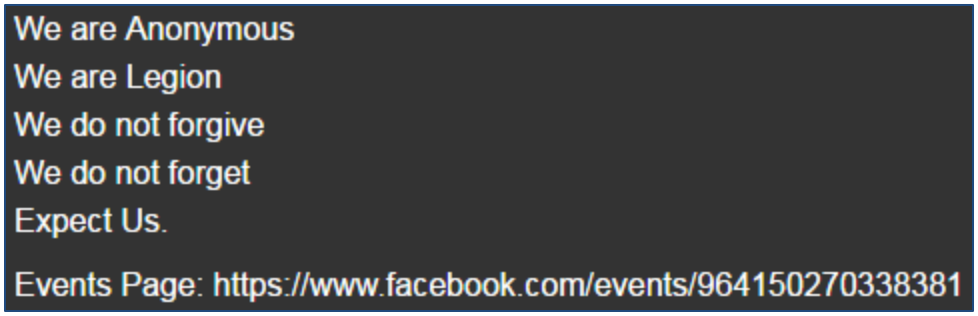
Les médias centrés sur l'actualité des technologies numériques et de la cybersécurité ont largement couvert durant le mois de mai 2016 la deuxième phase de la campagne hacktiviste #OpIcarus[2]. Cette dernière a pour objectif de dénoncer « *les travers engendrés par le système bancaire international* ». Les prémices de la campagne remontent à 2011 lorsque le collectif Anonymous souhaitait s'attaquer au New York Stock Exchange : « *Charge your lasers and aim them at the the New York Stock Exchange. (NYSE.com)* »[3]. De toute évidence, la première phase de #OpIcarus consistait à attaquer le site web de la plateforme d'échanges via des attaques DDoS. Cependant, l'opération ne rencontra pas un fort succès comme en témoigne le peu de retombées médiatiques mais également le faible nombre de vues (environ 3 700) de la vidéo mise en ligne en septembre 2011 sur YouTube[4].

La deuxième phase de l'opération fut amorcée à la fin du mois de janvier 2016, lorsque des membres apparemment affiliés au collectif Anonymous mirent en ligne un blog[5] anglophone appelé simplement « opicarus ». Ce dernier ne comporte qu'un seul et unique billet qui, lors de sa publication initiale, reprenait le texte du communiqué d'Anonymous de 2011 et proposait deux types d'action à mener dans le cadre de cette seconde phase. La première incitait les sympathisants à protester de manière physique le 8 février 2016 en face du siège du New York Stock Exchange et de la Banque d'Angleterre :

https://opicarus.wordpress.com/

2http://www.techworm.net/2016/05/anonymous-operation-opicarus-continues-ddoses-bank-cyprus.html
https://www.hackread.com/opicarus-hacktivists-shut-3-banking-websites/
http://www.infosecurity-magazine.com/news/anonymous-opicarus-bank-of-england/
http://www.ibtimes.co.uk/opicarus-anonymous-hacker-reveals-inspiration-behind-latest-operation-evolution-hacktivism-1561457
3 http://thehackernews.com/2011/03/operation-icarus-will-anonymous-shut.html
4 https://www.youtube.com/watch?v=NqA0Pqnleas
5 https://opicarus.wordpress.com/

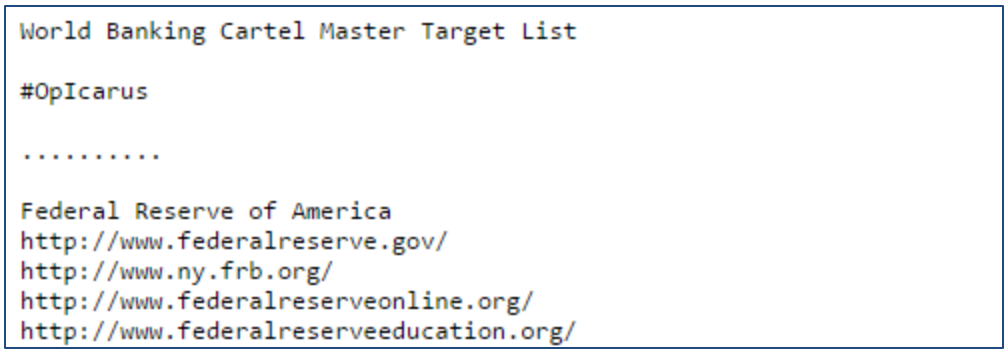
La deuxième action proposait de rejoindre une page d'un événement Facebook intitulé « OpIcarus 2016 Shut Down The Banks »[6] programmé pour le mois d'avril :



https://opicarus.wordpress.com/

Une initiative isolée relayée par le collectif officiel Anonymous

Cette page Facebook (toujours en activité), en plus de reprendre l'intégralité du billet publié sur le blog, propose plusieurs liens vers la plateforme YouTube où les vidéos expliquent les motivations sous-tendant la campagne #OpIcarus dans trois langues différentes : Allemand, Espagnol et Français. Le descriptif de l'événement est complété par un ensemble de liens vers des sites de type Pastebin[7] qui énumèrent près de 200 institutions financières à cibler par l'intermédiaire d'attaques DDoS contre leurs sites web :



```
World Banking Cartel Master Target List

#OpIcarus

.........

Federal Reserve of America
http://www.federalreserve.gov/
http://www.ny.frb.org/
http://www.federalreserveonline.org/
http://www.federalreserveeducation.org/
```

http://pastebin.com/y7JmsKVD

Il est intéressant de constater que le mouvement officiel Anonymous ne revendiqua pas à l'époque la mise en ligne du blog et encore moins le lancement d'une seconde phase #OpIcarus à l'encontre des organisations appartenant au secteur bancaire. Cette initiative ne fut relayée par Anonymous que bien plus tard, une fois les attaques lancées. En effet, le collectif ne communiqua officiellement qu'au début du mois de mai par l'intermédiaire de ses sites[8], de son groupe Facebook[9] et de sa chaine YouTube[10]. Il expliqua[11]

---

6 https://www.facebook.com/events/964150270338381

7 https://ghostbin.com/paste/cxhh5
https://nopaste.me/view/61113fc5

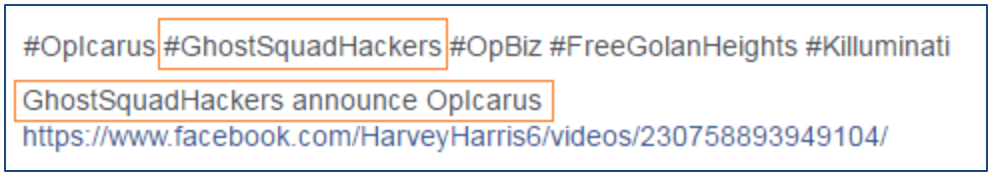
8 http://anonofficial.com/anonymous-operation-icarus-shut-down-the-banks-opicarus/

9 https://www.facebook.com/AnonymousDirect/posts/1720774338139566

10 https://www.youtube.com/watch?v=FYUjvbaj4bo

avoir rejoint l'initiative de groupes hacktivistes étant à l'origine de cette campagne, tels que le groupe Ghost Squad Hackers.

Ce dernier semble être l'une des organisations à l'origine de la création de l'événement Facebook « OpIcarus 2016 Shut Down The Banks », comme en témoignent certaines références présentes dans le descriptif :

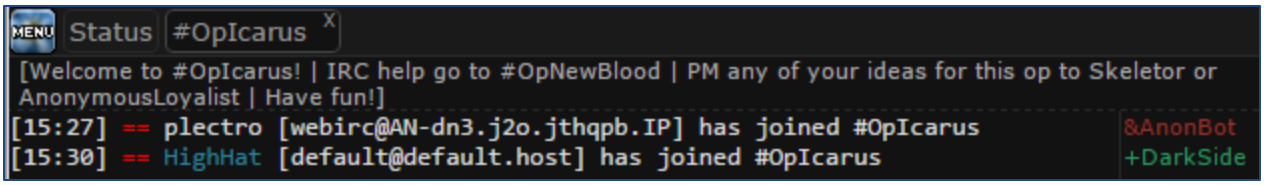


https://www.facebook.com/events/964150270338381

Les différents messages diffusés par le groupe lors de leurs précédentes campagnes de défacement et de planification d'attaques DDoS véhiculent clairement des idéologies pro-islam, anti-Israël, anti-État Islamique et surtout anti-capitaliste[12].

La seconde phase de la campagne #OpIcarus s'apparente donc à une initiative de groupes hacktivistes qui ne sont pas liés directement au collectif Anonymous en raison de divergences dans leur idéologie. Ils se rejoignent cependant sur l'anti-capitalisme, symbolisé par cette opération à l'encontre du système bancaire international.

Le canal officiel IRC d'Anonymous témoigne aussi de la position passive prise par le collectif dans l'organisation et la coordination de la campagne. En effet, les personnes souhaitant se joindre aux opérations trouvent traditionnellement un grand nombre d'informations – comme la liste des outils à utiliser ou des sites web à attaquer – directement sur le canal dédié à l'opération. Or, dans le cas présent, la seule indication pertinente est de rejoindre #OpNewBlood (le canal d'entrée pour les nouveaux membres Anonymous) ou de contacter un administrateur de la page via un message privé :



https://webchat.anonops.com/ Channel #OpIcarus

Environ 2000 personnes rejoignirent la page Facebook qui permettait de coordonner la campagne et ainsi de concentrer les efforts pendant la période du mois de mai.

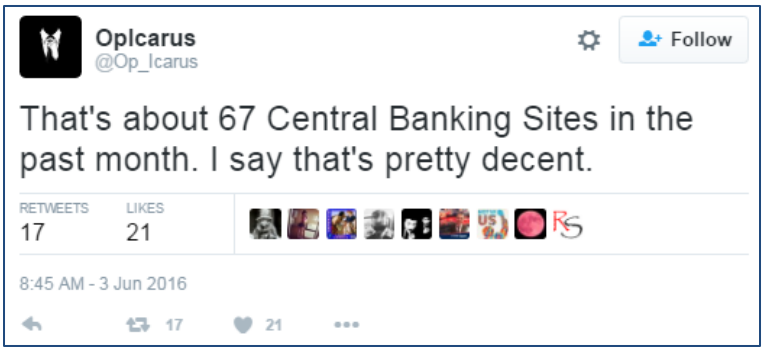
---

11 http://anonhq.com/opicarus-proceeds-hacktivism-shutdown-3-banks/
http://anonhq.com/opicarus-attacks-again/

12 https://www.facebook.com/GhostSquadHackers/photos
https://twitter.com/GhostSquadHack/media

Typologie des attaques : cibles impactées et outils utilisés

Les groupes impliqués dans #OpIcarus ont mené des attaques de type DDoS à l'encontre de leurs cibles de manière quotidienne tout au long du mois de mai 2016. Il n'est pas possible de confirmer si l'ensemble des institutions énumérées (un peu plus de 200) a été ciblé au cours de cette campagne de 30 jours. Cependant, les attaquants n'ont pas hésité à mettre en avant sur les réseaux sociaux leurs réussites, à savoir des sites web devenus inaccessibles à leurs utilisateurs. Ainsi, de nombreuses plateformes de banques majeures furent indisponibles suite aux attaques DDoS : Banque de Grèce, Banque Centrale de la République Dominicaine, Banque de Chypre, Guernsey Financial Services Commission, Banque Centrale du Monténégro, Banque Nationale du Panama, etc. Environ 67 sites web auraient été mis hors ligne durant le mois de mai :



https://twitter.com/Op_Icarus/status/738758438512152576

Contrairement aux attaques classiques d'origine hacktiviste, les attaquants ne se sont pas contentés de perturber la disponibilité des sites web vitrines des banques. Ils ont également visé des infrastructures, comme des serveurs de messagerie ou des distributeurs automatiques de billets. Le groupe Ghost Squad Hackers semble avoir particulièrement excellé dans ce domaine :

- Un membre dénommé s1ege endossa la responsabilité de l'attaque à l'encontre du serveur de messagerie de l'institution financière Bank of England :

https://twitter.com/_s1ege/status/730877442311770112

- Selon plusieurs publications sur des comptes Facebook, des distributeurs automatiques de billets de la banque Chase auraient également été rendus inopérants. Le compte Twitter officiel du support technique de la banque communiqua d'ailleurs sur le fait que leurs appareils rencontraient un problème au niveau du dépôt, sans mentionner l'origine de la panne :

https://twitter.com/chasesupport/status/731472017841590272

Cependant, le groupe Ghost Squad Hackers indiqua que cet incident faisait suite à une action intentée dans le cadre de #OpIcarus :

https://twitter.com/GhostSquadHack/status/731644936345559040

Les participants ont utilisé une variété d'outils de DDoS, la plupart non sophistiqués[13]. Il apparaît cependant que plusieurs groupes se sont appuyés sur des plateformes de type DDoS-as-a-Service, telles que des booters/stressers qui exigent un enregistrement et un paiement plus ou moins important selon la puissance de l'attaque demandée.

13 https://binarybin.org/413/

Cette deuxième phase de la campagne #OpIcarus permet de mettre en exergue plusieurs éléments sortant du cadre classique d'une campagne hacktiviste.

L'initiative de la deuxième phase de l'opération est à attribuer à des membres apparemment affiliés à Anonymous. Le collectif ne semble pas à l'origine de cette nouvelle étape de la campagne puisqu'il s'est clairement positionné en tant que relais. Ce phénomène témoigne de la montée en puissance d'un nouvel écosystème d'acteurs hacktivistes indépendants. Ces derniers sont structurés et possèdent de réelles capacités d'attaque. Ils sont dissociés d'Anonymous en raison de leurs idéologies et de leur radicalité mais trouvent une cause commune dans le cadre de certaines opérations.

Cette campagne est d'une grande ampleur puisqu'elle a eu un impact sur la disponibilité d'au moins 67 sites web d'institutions financières de renommée internationale mais a également visé des infrastructures importantes comme un serveur de messagerie et un réseau de distributeurs automatiques de billets. L'opération n'est pas éphémère, puisqu'elle a doucement débuté en janvier/février, puis s'est intensifiée au cours du mois de mai, et se poursuit encore aujourd'hui : #OpIcarus est entrée dans sa 3ème phase[14] et porte maintenant le nom de #ProjectMayhem en référence au film Fight Club[15].

14 http://anonhq.com/leak-anonymous-launches-opicarus-phase-3-project-hayhem/

15 https://www.facebook.com/OpIcarus2016/?fref=ts

UTILISATION ET DÉTECTION DES FAUX COMPTES SUR LES RÉSEAUX SOCIAUX

La plupart des institutions, partis, et professionnels de la politique ont recours aux réseaux sociaux dans leur stratégie de communication et disposent quasi systématiquement d'un compte officiel sur Twitter et Facebook. Ils ne sont cependant pas les seuls à s'appuyer sur ces plateformes. Les groupes terroristes ont également intégré le fait que l'utilisation des réseaux sociaux était le moyen de communication le plus efficient dans le développement de leur propagande.

Ce sont ainsi de véritables guerres d'influence qui sont menées à travers les réseaux sociaux. Elles disposent de leurs propres règles et codes, comme l'emploi massif des hashtags mais également la prolifération de faux comptes. Ces derniers font partie intégrante du paysage et sont utilisés par l'ensemble des acteurs. À titre d'exemple, seulement 35% des 500 millions de comptes Twitter seraient animés par des personnes réelles[16]. La problématique de la détection de ces faux comptes est donc centrale.

Vrai-faux profils et socialbots

Il existe différents types de faux comptes en raison des caractéristiques d'utilisation qui sont propres à chaque réseau social. Un **vrai-faux profil** Facebook n'est ni créé ni utilisé de la même façon qu'un **socialbot** Twitter.

Le cas de figure le plus récurrent sur Facebook est celui du **vrai-faux profil**. Ce ne sont pas des robots qui sont responsables de la création et de la gestion du compte mais bien des humains. Deux types sont présents sur la plateforme :

- Copie conforme d'un profil existant

Ce profil reprend le nom, les photos et l'entourage de la personne dont l'identité a été usurpée. Le but est d'utiliser la position de cette personne – qu'elle soit professionnelle, familiale, ou même amicale – afin d'abuser un proche. Recevoir un message d'une personne connue, possédant la photo de profil adéquate et les amis en commun correspondants, suscite un sentiment de confiance.

- Création d'un profil entièrement factice à partir d'informations tierces

Dans ce cas de figure, ce n'est pas l'identité complète d'un individu qui est usurpée. Le vrai-faux profil est composé de différentes informations (photos, nom, entourage…) appartenant à des individus distincts. Cette technique rend le compte plus crédible : les photos ne sont pas issues d'un magazine, l'entourage est homogène et des amis en commun reçoivent la même demande. À la différence de la première catégorie, il ne cible pas une personne en particulier.

Si sur Facebook la création de vrai-faux profils est le résultat d'une action humaine, sur Twitter les faux comptes sont principalement engendrés et gérés par des **socialbots**. Ces derniers sont des logiciels

16 http://www.nytimes.com/2013/08/11/sunday-review/i-flirt-and-tweet-follow-me-at-socialbot.html?_r=1

automatisés – ou robots – qui se propagent dans le but de convaincre les autres utilisateurs qu'ils sont des personnes réelles.

En règle générale, un socialbot est conçu pour pouvoir passer le test de Turing : il est suffisamment sophistiqué pour tromper les autres utilisateurs et ainsi être pris pour un être humain. Pour ce faire, le socialbot s'appuie sur l'intelligence artificielle, le « text mining » (qui est une technique permettant d'automatiser le traitement de gros volumes de contenus textuels) et l'analyse des données du logiciel. Certains socialbots ont accès à des bases de données de connaissances générales et s'appuient sur les événements actuels pour leur permettre de reconnaître les références et créer des messages plus convaincants[17].

Diplomatie-Digitale a déterminé cinq différents types de socialbots actifs sur Twitter[18]. Ils disposent de leurs propres caractéristiques, remplissent une fonction précise, et n'ont pas tous le même impact en termes d'influence stratégique :

- Le socialbot **relais**

Ce robot réagit à des mots clés, des hashtags ou à une expression particulière. Il se contente de « retweeter » ou de « favoriser » le tweet en question. Avec la répétition des tweets et l'identification des mots clés, ces socialbots sont très facilement reconnaissables et ne peuvent être confondus sur du long terme avec un réel compte Twitter possédé par un humain. De ce fait, son interaction avec les autres comptes Twitter est minimale.

- Le socialbot **pourvoyeur**

Le socialbot pourvoyeur est un robot qui réagit de la même façon que les socialbots relais mais il est plus puissant et plus fiable. Il emploie des algorithmes bien plus avancés que le socialbot relais, s'appuyant sur les API de différents web services. Il est capable de faire une veille utile à partir d'un mot clé, d'un hashtag ou d'une expression.

- Le socialbot **spammeur**

Ce robot est très peu complexe d'un point de vue technologique mais il est plus redoutable en termes d'efficacité quand il s'agit de répandre en masse des informations.

- Le socialbot **follower**

Ce robot représenterait plus de 45% des comptes qui suivent les entreprises sur Twitter. Il se contente de suivre les comptes de certaines marques (qui ont payé pour, et ainsi accroitre leur notoriété/visibilité) ou de retweeter les publications de ces entités. Du fait de sa nature, il est facilement détectable.

17 https://www.techopedia.com/definition/27811/socialbot

18 http://www.diplomatie-digitale.com/featured/strategie/robots-et-reseaux-sociaux-etat-des-lieux-prospectives-783

- Le socialbot **influenceur complexe**

Ces socialbots sont les plus élaborés techniquement parlant. Ils sont suffisamment performants pour gagner de la notoriété « en leur nom propre ». Très difficiles à identifier, ils sont dotés d'une intelligence artificielle leur permettant de tenir une discussion intelligible, de réagir d'une façon semblable à un humain ainsi que de propager une idéologie.

Ces socialbots peuvent avoir une influence différente en fonction de leur utilisation. En termes d'influence stratégique, le socialbot influenceur complexe est le plus performant et le moins facilement détectable.

La difficile détection des faux comptes sur les réseaux sociaux

En raison de leur fonctionnement différent, les vrai-faux profils Facebook et les socialbots Twitter ne se détectent pas de la même manière.

La détection des socialbots Twitter :

En 2011, une équipe de chercheurs de l'université Texas A&M University a développé un algorithme dans le but de repérer les socialbots sur Twitter. Le principe de cette technique était de créer une sorte d'appât («honeypot») ne pouvant être détecté que par les comptes robots au vu de l'absurdité du contenu du tweet. Les comptes qui réagissaient à ce tweet (via le suivi du compte émetteur, l'ajout du tweet en favoris ou bien le retweet) étaient alors répertoriés en tant que robots[19]. L'équipe a donc rédigé 60 tweets honeypots qui ont agglomeré plus de 30 000 comptes Twitter considérés comme étant des socialbots. Ces derniers étaient principalement des socialbots relais ou pourvoyeur. Cette étude effectuée en 2011 a montré ses limites en raison du développement de nouveaux socialbots bien plus avancés technologiquement tels que les socialbots influenceurs complexes.

C'est à l'Université d'Indiana à Bloomington qu'Emilio Ferrara et son groupe de recherche Truthy ont mis au point un système leur permettant de détecter les socialbots dotés d'une grande intelligence artificielle. L'équipe de M. Ferrara a collecté l'ensemble des socialbots détectés lors de l'étude préalablement faite par les universitaires texans. Parmi les 35 000 socialbots relevés, seuls 15 000 ont été étudiés. L'équipe a analysé les 200 derniers tweets de ces comptes ainsi que les 100 tweets les plus récents les mentionnant. Une base de données a alors été constituée avec plus de 2,6 millions de tweets. Cette même démarche a été effectuée pour 16 000 utilisateurs humains avec 3 millions de tweets. Après avoir constitué cette base de données, les chercheurs ont créé un algorithme appelé *Bot or not ?*[20]. Le but de ce dernier était de rechercher les différences significatives entre les utilisateurs humains et les robots grâce à l'analyse de plus de 1 000 caractéristiques associées tels que le nombre de tweets et retweets, le nombre de réponses, la mention de compte, la longueur du nom d'utilisateur, ou encore l'âge du compte.

Des différences significatives sont alors apparues :

- Les socialbots retweetaient beaucoup plus souvent que les humains,

19 https://www.technologyreview.com/s/529461/how-to-spot-a-social-bot-on-twitter/

20 http://truthy.indiana.edu/botornot/

- Le nom d'utilisateur des socialbots était plus long que la moyenne des comptes d'utilisateurs humains,
- Les humains recevaient plus de réponses à leurs tweets et étaient bien plus mentionnés dans les comptes des autres utilisateurs.

L'ensemble de ces éléments permit de constituer une sorte d'empreinte digitale pour détecter des socialbots. Mais cette technique comporte également des limites. La première porte sur l'échantillon de base : se basant sur les bots détectés lors de l'étude de 2011, les chercheurs exclurent la possibilité de l'existence de bots bien plus performants. De plus, ce test excluait également la possibilité d'emprunt de comptes réels par des robots (voir exemple de « L'Aube de la Bonne Nouvelle » ci-dessous) et inversement.

Mais la plus grande limite à ce test fut le concept propre de Twitter : un message en 140 caractères maximum. Cette restriction permet d'imiter le comportement humain bien plus facilement que lorsque les caractères ne sont pas limités (comme sur Facebook). De plus, il n'est nul besoin de créer une identité réelle et les messages peuvent être lus par l'ensemble des utilisateurs de Twitter ; contrairement à Facebook dont le concept est que l'utilisateur publie des éléments qui ne peuvent être lus que par les personnes acceptées et autorisées à accéder à ces contenus.

La détection des vrai-faux profils Facebook :

La détection des faux profils Facebook est un réel problème et il n'existe pas d'outils permettant d'analyser la fiabilité d'un profil. En revanche, de nombreux tutoriels détaillent une technique manuelle permettant une analyse plus ou moins fiable d'un compte Facebook en prenant en compte différentes caractéristiques :

- Les photos : il faut analyser les photos, leur nombre, les commentaires et les « likes » qu'elles ont reçues. Une recherche via Google et sa fonction « recherche inversée d'images » permet également de savoir d'où a été obtenue la photo ;
- Les amis : il faut analyser le nombre d'amis de la personne et leurs interactions afin de déterminer si ces amis sont réels ou simplement de « vrai-faux profils » ;
- L'orthographe : la syntaxe va permettre d'analyser le profil de la personne. En cas d'usurpation d'identité, il suffit de comparer avec la précédente page Facebook de l'individu. En revanche, si la personne est inconnue, il est facile de détecter des fautes qui ne peuvent être commises que par des personnes non françaises comme une erreur dans le déterminant (exemple : « le amour », « le ordinateur »).

Plusieurs tutoriels expliquent également quelles questions pièges il est utile de poser afin d'analyser si une page Facebook est vraiment ce qu'elle prétend être (questions précises de géographie). Le but est de piéger la personne sur ce qu'elle affirme être.

Les socialbots et l'influence stratégique

Les socialbots ont démontré par le passé leurs réelles capacités d'influence. Plusieurs exemples concrets illustrent ce fait.

L'exemple le plus significatif d'un socialbot influenceur complexe ayant réussi sa mission est celui créé par des chercheurs de l'Université fédérale d'Ouro Preto en 2011. Le but de ce socialbot était de démontrer que

les mesures d'influence effectuées par Twitter n'étaient pas fiables. Ils ont donc créé un bot nommé Carina Santos (@Scarina91). Ce compte Twitter avait été programmé avec différentes caractéristiques censées le rendre plus crédible. Le compte devait tout d'abord systématiquement arrêter de « suivre » ceux qui ne le suivaient pas en retour au bout de quelques jours. Quant aux contenus, « la journaliste » ne devait poster que des informations liées à l'actualité. De plus, afin d'éviter de paraître trop stéréotypé, les chercheurs ont programmé le compte @Scarina91 afin qu'il recherche sur Twitter les tweets qui traitaient de l'actualité dans le monde. Une fois trouvés, soit le bot copiait les tweets, soit il les retweetait. Les chercheurs ont également programmé le compte afin qu'il distribue des tweets à un rythme varié, recréant l'activité Twitter d'un être humain[21].

Twitalyzer, qui était un outil de mesure d'influence stratégique, avait déterminé que ce compte Twitter était plus puissant en termes d'influence que celui d'Oprah Winfrey…

Autre exemple : l'application « L'Aube de la Bonne Nouvelle » (The Dawn Of Glad Tidings) lancée par l'Etat Islamique en 2014. Avec cet outil, le groupe terroriste met en pratique sa stratégie de communication : être audible, répandre son idéologie et recruter via des canaux de communication non traditionnels (communiqués de presse, journaux télévisés, rencontres diplomatiques, etc.)[22]. Pour un groupe tel que l'EI, les réseaux sociaux sont ainsi une porte d'entrée sur le monde. Une fois l'application téléchargée sur Google Play Store, il suffisait de connecter un compte Twitter sur l'application qui en prenait le contrôle et twittait automatiquement des contenus à la place de l'utilisateur. Le 10 juin 2014, lors de la prise de Mossoul, l'application posta plus de 40 000 tweets en une journée via les comptes Twitter des individus l'ayant téléchargé et installé. Cette application est un bon exemple de robot prenant le contrôle de vrais comptes Twitter.

L'appellation « faux comptes » recèle cependant différentes nuances. On ne peut détecter de la même façon un vrai-faux profil Facebook qui usurpe l'identité de quelqu'un et un socialbot influenceur complexe. La démarche de vérification effectuée par l'humain est aujourd'hui considérée comme étant la démarche la plus efficace dans la détection des faux comptes Facebook, étant donné que ces comptes sont eux-mêmes opérés par des humains. En revanche, concernant les socialbots présents sur Twitter, l'ouverture de la plateforme et les données massives générées par ces comptes facilitent le développement d'algorithmes permettant de les détecter. Ce type d'outil sort tout juste du cadre universitaire et certaines entreprises privées comme Proofpoint ou LookingGlass Cyber Solutions sont aujourd'hui présentes sur le marché de la sécurité des « réseaux sociaux ». Cette dernière propose notamment des outils de détection des faux profils[23].

21 http://www.dailydot.com/news/new-twitter-bots-klout-score-test/

22 https://rslnmag.fr/cite/les-reseaux-sociaux-une-nouvelle-arme-de-guerre/

23 https://www.proofpoint.com/us/corporate-blog/post/dont-let-angler-phishing-lure-customers-into-trap

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la Défense et des Anciens combattants
Direction Générale des Relations Internationales et de la Stratégie
14 rue Saint-Dominique - 75700 – Paris SP 07

CEIS
280 Boulevard Saint-Germain - 75007 - Paris
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com