Lettre mensuelle – Septembre 2019 - disponible sur omc.ceis.eu

Table des matières

ANALYSES

1. GÉOPOLITIQUE DE LA BLOCKCHAIN

Le protocole blockchain a été créé en 2008, par un inconnu retranché derrière le pseudonyme de « Satoshi Nakamoto », à une période caractérisée par une défiance croissante envers le système bancaire et financier. S. Nakamoto a alors publié un document de neuf pages présentant l'architecture technologique de la cryptomonnaie Bitcoin en expliquant qu'« une version purement pair-à-pair de l'argent électronique permettrait aux paiements en ligne d'être envoyés directement d'une partie à l'autre sans passer par une institution financière ». La vocation première de la blockchain était ainsi de supprimer les intermédiaires (banques, administrations, régulateurs) dans les échanges financiers, dans un contexte post-crise économique et financière de 2007-2008.

FOCUS : LA BLOCKCHAIN C'EST :

- ***La combinaison de 3 briques technologiques :***

- Une architecture « peer-to-peer » (P2P) : chaque ordinateur/utilisateur est à la fois client et serveur, et peut échanger directement sans transiter par un serveur central.
- Une fonction de *hashage*, qui permet d'attribuer à chaque donnée une empreinte numérique unique qui l'identifie.
- La Cryptographie asymétrique : qui repose sur un système à double clé de chiffrement, privée et publique.

- ***Une garantie de sécurité dans toutes ses dimensions :***

- La disponibilité des informations, garantie par le caractère décentralisé du modèle et par la technologie P2P sur laquelle il s'appuie, qui permet de consulter l'historique des transactions sur chaque nœud du réseau.
- La traçabilité, via l'horodatage des transactions sur un registre distribué consultable par tous, donnant la possibilité de remonter la chaîne pour en retrouver l'historique.
- L'intégrité et l'inviolabilité grâce à l'inscription dans un bloc de transactions qui ne peut pas être écrasée et devient ainsi infalsifiable et facilement vérifiable.
- La confidentialité, assurée par l'usage du pseudonymat et d'une technologie algorithmique basée sur une cryptographie de haut niveau combinant chiffrement asymétrique et fonction de *hashage* SHA -256.

En quelques années, la blockchain est passée du stade de technologie émergeante à celui de technologie révolutionnaire, au point d'être consacrée « Méga tendance » par le World Economic Forum en 2015. Rapidement, le nombre d'applications et d'usages a crû, dans une multitude de domaines. La blockchain a alors atteint le « pic des attentes exagérées » de la courbe du Hype de Gartner, dans un contexte d'emballement médiatique. Ces dernières années, le nombre d'applications basées sur la blockchain semble cependant décroître. La blockchain est aussi moins présente dans les médias. La technologie semble avoir

atteint le « gouffre des désillusions », où la réalité des produits déçoit. La blockchain n'a toutefois pas totalement disparu du paysage technologique. Si elle continue de faire parler d'elle cela est cependant moins en termes de progrès et d'innovation, signe que son succès dépasse le simple cadre de la technologie, que d'impact sur certains enjeux de sécurité intérieure, de stabilité internationale et d'empreinte écologique et économique.

FOCUS : principaux usages et applications

- ***Un moyen de paiement décentralisé*** *:* Les crypto-monnaies se comptent par centaines dont *Bitcoin*, la plus sérieuse et établie, ou encore *Monéro*, *Namecoin*, *Ripple*, *Dash...* Elles permettent d'effectuer, rapidement à moindre coût, des transferts monétaires désintermédiés (sans transit par les établissements bancaires et financiers) dont les références sont stockées sur un grand registre distribué et auditable.

- ***Les smart contracts***, des contrats auto-exécutants qui se déclenchent automatiquement à la réalisation de certaines conditions d'engagement, sur la base d'un ensemble des conditions et limitations programmées dans le contrat à l'origine. Des projets à l'étude envisagent des applications pour la gestion et la compensation des retards dans les transports.

- ***Enregistrement et traçabilité de biens de valeur,*** dont les caractéristiques sont enregistrées sur une blockchain publique, devenant ainsi infalsifiables et facilement traçables. Cette application est déjà en usage pour les diamants, les pur-sangs, les œuvres d'art, les vins d'exception…

Par soucis de clarté, les analyses présentées ci-dessous se basent essentiellement sur les blockchains publiques (cf. encart ci-dessous).

FOCUS : Les trois types de Blockchain

- Les **blockchains publiques** (comme la cryptomonnaie Bitcoin) sont ouvertes à tout individu *via* Internet. La validation des transactions repose sur la notion de consensus décentralisé, affranchi d'une autorité centrale de contrôle.
- Les **blockchains privées** sont soumises à des barrières à l'entrée et à une gouvernance centralisée. Les participants doivent être acceptés par l'entité qui l'administre. C'est cette entité centrale qui définit les règles de fonctionnement.
- La **blockchain hybride** est une blockchain dont la gouvernance est partiellement décentralisée entre plusieurs entités qui forment un consortium. L'accès y est donc limité et la validation des transactions fonctionne souvent avec des règles de type « vote majoritaire ».

1) La blockchain, menace pour la sécurité intérieure et la stabilité internationale ?

a) La blockchain au service de la criminalité organisée

En supprimant les intermédiaires institutionnels dans les transactions, notamment financières dans le cadre des cryptomonnaies, la blockchain se révèle ambivalente : échappant au contrôle des autorités et aux circuits traditionnels et régulés des échanges économiques et financiers, elle peut ainsi faciliter la **criminalité** (blanchiment d'argent, évasion fiscale, financement de trafics de drogue, d'armes, de cartes de crédit volées, etc.), voire le financement du **terrorisme**. A titre d'exemple, en 2016, la police néerlandaise a arrêté 10 individus accusés de blanchir de l'argent via la vente de cryptomonnaies. D'autant que les échanges et transactions effectués via une blockchain sont réalisés sous pseudonyme, ce qui rend l'identification des protagonistes très difficile (bien que possible) et favorise les activités illicites impliquant des crypto-monnaies, notamment sur le dark web. A noter toutefois que l'utilisation de la blockchain à des fins criminelles à travers les cryptomonnaies reste relativement limitée : en 2019, seulement 0,5% du total des transactions en Bitcoin (soit $829 millions de dollars) aurait été dépensé sur le dark web[1].

Certains **groupes terroristes**, toutefois relativement isolés, tentent également d'utiliser le Bitcoin, adossé à la blockchain, pour financer leurs activités. Récemment, en janvier 2019, les brigades Izz ad-Din al-Qassam, branche du Hamas, auraient lancé une campagne de financement par le Bitcoin[2]. Des groupes djihadistes, comme al Sadaqah et Jahezona, auraient également eu recours à des campagnes de levée de cryptomonnaies[3]. Ce mode de financement présente cependant des limites et le volume des fonds récoltés pendant ces campagnes est dans les faits très restreint. La campagne menée par le groupe al Sadaqah n'a par exemple récolté que 1 037 de dollars en un an et demi. Les transactions relatives au Hamas, qui ont atteint près de 1 000 de dollars en quelques jours, ont toutefois été tracées par un logiciel de suivi développé par la société d'investigation en cybercrime Elliptic, ce qui a permis d'identifier les régions -Europe et Etats-Unis- d'où étaient envoyés les fonds[4].

b) La blockchain, outil de pression diplomatique

Comme l'a montré l'essor de la blockchain dans le contexte post-crise financière de 2008, cette technologie peut être perçue comme un indicateur de défiance, voire de rejet, envers les autorités étatiques. Paradoxalement, certains États utilisent aujourd'hui eux-mêmes la blockchain : de cette façon, ils s'approprient une technologie initialement conçue pour les contourner. Trois exemples récents sont particulièrement parlants :

- **Vénézuela** : un média espagnol[5] a montré que le gouvernement Maduro utilisait un portefeuille digital pour transformer en cryptomonnaies les recettes issues des taxes des aéroports domestiques. Les actifs digitaux sont ensuite transférés à Honk-Kong, en Chine, en Russie et en Hongrie, où ils sont convertis en

[1] https://www.elliptic.co/our-thinking/bitcoin-money-laundering

[2] https://www.elliptic.co/our-thinking/countering-terrorist-financing-cryptocurrency

[3] https://www.justice.gov/opa/pr/new-york-woman-pleads-guilty-providing-material-support-isis

[4] https://www.elliptic.co/our-thinking/countering-terrorist-financing-cryptocurrency

[5] https://www.abc.es/internacional/abci-maduro-tasas-aeroportuarias-para-burlar-sanciones-eeuu-201907212232_noticia.html

monnaie réelle et re-transferés sur les comptes publics du Venezuela. Cette manœuvre permet aux autorités vénézuéliennes de contourner les sanctions économiques.

- **Russie et Turquie** : en décembre 2017, les deux pays ont réalisé un échange commercial uniquement grâce au Bitcoin[6].
- **Iran** : le pays a lancé en juin 2019 sa propre cryptomonnaie, adossé à la réserve d'or iranienne, afin de tenter de contourner les sanctions américaines[7].

Ces 4 pays plus la Chine, parfois qualifiés de « crypto rogue states[8] », semblent vouloir utiliser les cryptomonnaies -et donc la blockchain à laquelle elles s'adossent- pour réaliser des échanges commerciaux en dehors du système économique et financier (et de ses sanctions) dominé par les États-Unis. Ainsi, la blockchain et les cryptomonnaies s'immiscent dans les rapports de force interétatiques. Elle permet à certains États de contourner l'influence d'autres États et de s'affranchir de certaines régulations ou sanctions, avec potentiellement deux impacts conséquents : une modification de l'ordre monétaire global d'une part, et la déstabilisation de l'ordre géopolitique en cas d'aggravation de situations déjà tendues d'autre part, entre le Venezuela et les Etats-Unis, ou entre l'Iran et les États-Unis par exemple.

2) La blockchain, une réponse aux grands enjeux politiques et géopolitiques

a) Un outil de lutte contre la (cyber)criminalité ?

Comme évoqué précédemment, la blockchain est particulièrement attractive pour les criminels qui peuvent se cacher derrière un pseudonyme, parfois en passant par plusieurs intermédiaires. Si retracer des cybercriminels utilisant la blockchain reste dans les faits un exercice difficile et si certains ne sont jamais démasqués, le pseudonymat ne permet qu'une protection partielle, offrant une brèche exploitable par les cellules d'investigation. Les forces de sécurité ont parfois recours aux services des comptoirs de change ou de certaines sociétés pour tenter de retrouver les auteurs de transactions douteuses, frauduleuses ou criminelles. La start-up **Scorechain[9]**, issue de la société luxembourgeoise Neofacto, a par exemple développé un outil de lutte contre le blanchiment d'argent. La solution s'adresse aux banques, aux sociétés d'audit et aux crypto-courtiers. Elle les aide à détecter les activités frauduleuses grâce au suivi et à l'analyse des transactions en cryptomonnaies. La société britannique **Elliptic[10]** propose quant à elle des services d'investigation en cybercriminalité en coopération avec les autorités compétentes. Elliptic a développé un logiciel qui aide les investigateurs à relier l'identité digitale (pseudonyme) des utilisateurs de la blockchain du Bitcoin à leur identité réelle. Cette solution est déjà utilisée par des services britanniques et américains dans le cadre d'enquêtes sur le rôle de Bitcoin dans des affaires de trafic de stupéfiants, d'images pédopornographique, et de ransomware.

[6] https://steemit.com/bitcoin/@stayoutoftherz/first-cryptocurrency-freight-deal-takes-russian-wheat-to-turkey
[7] https://www.ccn.com/iran-punks-trump-crypto/
[8] Référence aux *rogue states*, ou Etats voyous, désignés comme tels par les Etats-Unis du fait -entre autres- du caractère dictatorial de leur régime, de leur participation à la prolifération des armes de destruction massive et de leur atteinte à la sécurité internationale. La Libye, Cuba, la Corée du Nord, l'Irak, l'Iran et la Syrie font notamment partie des Etats considérés comme voyous par les Etats-Unis.
[9] https://www.scorechain.com
[10] https://www.elliptic.co

b) Combler les lacunes d'(infra)structures sociales manquantes ou défaillantes

La blockchain est également utilisée pour combler des lacunes étatiques et/ou sociales. Une start-up basée au Texas a par exemple signé un accord avec le gouvernement du Honduras pour la mise en œuvre d'un **cadastre numérique basé sur la blockchain**[11]. Le système foncier hondurien est en effet rendu inefficace par une importante fraude à la propriété. Des fonctionnaires de l'Etat auraient comme habitude d'accéder illégalement au registre du cadastre pour s'attribuer les propriétés de leur choix. De plus, la plupart des propriétaires ne se sont jamais inscrits au cadastre. L'idée d'un registre numérisé et basé sur une blockchain est d'encourager les propriétaires à s'enregistrer en leur assurant la sécurité de leur titre de propriété.

2. LES BOTNETS, DE LA CYBERCRIMINALITÉ À LA DÉFENSE CYBER

En juillet 2019, la Gendarmerie nationale neutralisait Retadup, un botnet à l'origine de la compromission d'au moins 1,3 millions d'ordinateurs, ce qui en fait l'un des plus importants au monde identifiés à ce jour. Cette opération, une première en France et, à bien des égards, au niveau mondial, a suscité un regain d'attention pour cette forme de cybermenace.

Un botnet désigne un réseau de machines compromises par un malware (les bots[12]) et contrôlées à distance par un individu malveillant (le botmaster). Pouvant les actionner à sa guise par l'intermédiaire d'un serveur de Command and Control (C&C, CC ou C2), le botmaster transmet des ordres – à l'insu des véritables propriétaires des machines – à une partie ou à la totalité des bots.

Si l'actualité a surtout mis en lumière l'utilisation des botnets à des fins de cybercriminalité, ils peuvent aussi trouver une place en soutien aux opérations militaires. Leur capacité à accroître les effets d'une opération de cyberdéfense permettent en effet aux botnets de trouver une application dans la poursuite des trois objectifs opérationnels décrits par la doctrine de lutte informatique offensive[13] : recueil ou extraction d'informations, réduction ou neutralisation des capacités adverses, ainsi que modification des perceptions ou de la capacité d'analyse de l'adversaire.

ARCHITECTURES D'UN BOTNET

Les botnets ont, au fil du temps, évolué pour adopter différents types d'architectures, de façon à trouver le meilleur équilibre entre contrôle des bots, conservation de l'anonymat des botmasters, et résilience du réseau. Ainsi, les botnets peuvent s'appuyer sur une architecture centralisée (figure 1), par procuration (figure 2) ou Peer-to-peer (figure 3).

[11] https://www.reuters.com/article/usa-honduras-technology/honduras-to-build-land-title-registry-using-bitcoin-technology-idINKBN0O01V720150515?irpc=932 ; https://www.reuters.com/article/us-honduras-landrights-tech/modernizing-land-records-in-honduras-can-help-stem-violence-says-analyst-idUSKBN1AR151

[12] Les bots informatiques sont des agents logiciels automatiques ou semi-automatiques qui interagissent avec des serveurs informatiques de la même façon que le feraient des programmes clients utilisé par des humains.

[13] Ministère des Armées, *Éléments publics de doctrine militaire de lutte informatique*, DiCoD, p.6.

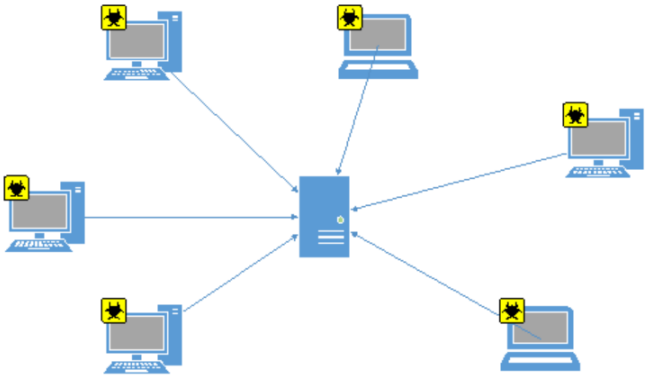

Figure 1 Central C&C server

Source : Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)

L'architecture centralisée ou « en étoile » est la plus simple à mettre en place : toutes les machines et composantes du réseau sont reliés à un système central chargé d'assurer la communication entre eux. Contreparties de sa simplicité : il suffit de couper le serveur C&C central pour que l'intégralité de ce système tombe et il est plus facile et plus rapide de remonter jusqu'au botmaster.

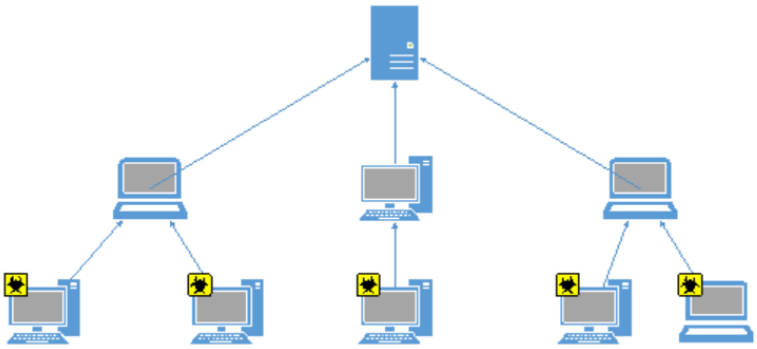

Figure 2 Proxied C&C

Source : Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)

L'architecture par procuration (ou « par proxy ») est en de très nombreux points similaire au modèle précédent, à la différence toutefois que les nœuds du réseaux ne communiquent pas directement avec le serveur central mais transitent par des nœuds intermédiaires, qui peuvent être des serveurs opérés par le botmaster ou des machines elles mêmes infectées. L'interruption d'un nœud interméditaire entraine la perte d'une partie du réseau seulement, sans mettre en danger l'ensemble : elle est donc plus résiliente. Avec cette architecture il est également plus long de remonter jusqu'au botmaster.

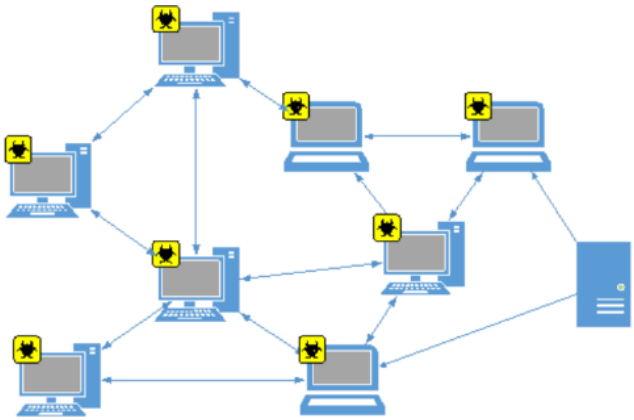

Figure 3 Peer-to-peer botnet

Source : Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)

L'architecture peer-to-peer est la plus décentralisée : dans cette configuration, chaque client est également serveur, ce qui rend le système plus résilient et allonge le délai pour remonter de nœud en nœud jusqu'au botmaster, bien plus conséquent que dans les deux modèles précédents. En s'abritant derrière une multitude de nœuds et donc d'adresses IP, le botmaster conserve également un haut niveau d'anonymat, ce qui en fait le modèle le plus couramment utilisé dans les architectures de botnet.

LES BOTNETS, AMPLIFICATEURS DE CYBER-ATTAQUES

Un botnet peut contrôler des milliers voire des millions de machines – Retadup en contrôle au moins 1,3 million[14] – ce qui permet au botmaster d'intensifier l'impact et l'envergure de ses cyber-opérations de façon significative, en multipliant leurs effet par le nombre de bots qu'il a sous son contrôle.

Outre des campagnes massives de spams ou de vols de données, ce mécanisme d'amplification[15] est le plus souvent utilisé à des fins d'attaques par déni de service distribué (DDoS). La cyberattaque lancée par des hackers russes sur l'Estonie en avril et mai 2007 est certainement l'exemple le plus probant du potentiel amplificateur et de l'impact que peut avoir un botnet sur la sécurité d'un État. Une campagne d'attaque DDoS lancée en réponse à une décision politique jugée contraire aux intérêt russes par le gouvernement estonien (en l'occurrence, le déplacement d'un mémorial soviétique) a obligé certaines administrations estoniennes (dont la Défense) à couper l'accès de leur site Internet aux adresses IP étrangères pendant plusieurs jours.

Il est intéressant de noter que l'accès à cette capacité offensive que constituent les botnets s'est largement démocratisée et peut aujourd'hui être utilisée dans le cadre d'une « location » sur des plateformes en ligne où le prix d'une attaque DDoS varie selon son intensité. Recourir à un botnet pour une utilisation ponctuelle ne nécessite ainsi plus d'expertise technique spécifique et constitue pour le botmaster une activité lucrative[16]. Coordonnée notamment par Europol, l'opération Power OFF a démantelé en avril 2018 les activités du

[14] « Botnet neutralisé: comment la gendarmerie française a opéré », *Le Point*, 25 septembre 2019.
[15] J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, *Les Manipulations de l'information : un défi pour nos démocraties*, rapport du CAPS (MEAE) et de l'IRSEM (MINARM), Paris, août 2018, p. 85.
[16] Brian Prince, « Botnets for Sale Business Going Strong, Security Researchers Say », *eWeek*, 25 octobre 2010.

site« webstresser.org », à l'origine de plus de 4 millions d'attaques DDoS. Ce dernier louait des attaques DDoS à partir de 15 euros et comptait 151 000 utilisateurs[17].

Parfois qualifié de « bombe atomique » ou de « porte-avions »[18] du cyberespace, le potentiel de cette véritable « force de frappe » ne se limite pas à ses capacités de destruction, et ce alors qu'elle serait en mesure neutraliser les infrastructures critiques d'un Etat, comme le suggèrent les « avertissements » lancés par la Russie en Estonie en 2007, ou à la Géorgie en 2008. Dans le cadre d'une cyberopération, le botnet permet surtout à son utilisateur de densifier ses moyens d'action aux niveaux stratégique et tactique[19].

LES BOTNETS AU SERVICE DE CYBER-OPÉRATIONS OFFENSIVES

Les botnets sont régulièrement utilisés dans le cadre de cyber-opérations menées par des Etats ou servant des intérêts étatiques. Les opérations d'APT28[20], un groupe russe de pirates informatiques connu pour aligner ses campagnes et ses cibles sur les intérêts du Kremlin, ont été largement étudiées ces derniers mois.[21]

Dans ces derniers cas, les botnets ont pu être utilisés dans divers contextes :

Recueil ou extraction d'informations

Les botnets dotés d'un logiciel espion (« spyware »),tels que des enregistreurs de frappe (keylogger), ou chevaux de Troie, peuvent être utilisés à des fins de renseignement, pour recueillir des informations sur un adversaire (adresses courriels, opérations en cours ou futures) et ainsi mieux évaluer ses capacités. Une multitude d'autres outils permettent également au botmaster d'extraire ponctuellement des données à partir de ses bots, qui peuvent être utilisés comme des « cellules dormantes » : capture d'écran, caméra, logiciels publicitaires (*adware*), et les cookies pour les données personnelles[22].

On attribue par exemple à APT28[23] la cyberattaque par spear-phising contre[24] le collectif féministe *Pussy Riot*, opposé à la politique de Vladimir Poutine, ou la supposée interception du trafic email du ministère kirghize des Affaires étrangères en 2015, dans le cadre d'opérations visant à recueillir du renseignement.. Membres de l'équipe de campagne de l'américaine Hillary Clinton, son directeur John Podesta et William Rinehart auraient également été ciblés par le groupe à l'occasion des élections présidentielles de 2016.

Plus récemment, dans une opération de 2017 ciblant le secteur de l'hôtellerie en Europe et au Moyen-Orient, le groupe APT28 se serait introduit dans le réseau de l'enseigne ciblée, via un document malicieux envoyé

[17] « Authorities across the world going after users of biggest DDoS-for-hire website », *Europol*, 28 janvier 2019.
[18] *Cybercriminalité : les gendarmes neutralisent le botnet géant "Retadup"*, France 24 (Youtube), 28 août 2019.
[19] Eric Koziel, David Robinson, « Botnets as an Instrument of Warfare », *5th International Conference Critical Infrastructure Protection (ICCIP)*, Mars 2011, États-Unis, p. 20.
[20] Aussi connu sous les noms de Fancy Bear, Swallowtail, Pawn Storm, Sofacy Group, Sednit, Strontium et Tsar Team.
[21] Il est important toutefois de noter qu'APT28 n'a pas l'exclusivité de ce type d'opérations et que d'autres groupes utilisent les botnets ou poursuivent le même genre d'objectifs.
[22] Zsolt Bederna, Tamas Szadeczky, « Cyber espionage through Botnets », Security Journal, Palgrave Macmillan, 2019.
[23] « APT28 : au cœur de la polémique », FireEye, 2017.
[24] Campagne de phishing ciblée

par e-mail, et se serait propagé dans ses réseaux pour compromettre les ordinateurs de ses clients et exfiltrer des ordinateurs des données telles que noms, identifiants et mots de passe.

Réduction ou neutralisation des capacités adverses

Technique de sabotage informatique[25], une attaque DDoS peut aussi permettre de paralyser les activités essentielles d'un État (blocage des services publics en ligne, télécommunications, activités bancaires, médias, etc.) et fragiliser ses infrastructures critiques. Par l'intermédiaire du botnet Mirai#14, un hacker britannique a ainsi conduit en 2015 plusieurs attaques DDoS sur Lonestar, principal opérateur du Libéria, qui ont fini par priver le pays d'accès à Internet pendant une journée et affecter le fonctionnement du réseau pendant plusieurs semaines.[26].

Si l'utilisateur malveillant peut s'appuyer sur un réseau de botnets assez vaste qui lui confère une force de frappe suffisante, il peut opter pour une approche type « démonstration de force[27] , une opération consistant en une série attaques qui vont crescendo et s'intensifient dans l'espoir de faire céder un adversaire, par exemple le faire accéder à des revendications politiques. Une campagne de neutralisation des infrastructures critiques via un botnet ainsi peut ainsi trouver sa place dans l'arsenal de mesures de cyberdéfense à la dispositions des Etats et des armées et être combinées à d'autres outils, plus traditionnels, dans le cadre d'opérations militaires.

Les attaques DDoS sont très souvent utilisées couplées à un réseau de botnets, d'abord car elles en sont d'abord plus efficaces car amplifiées, ensuite parce que ce dispositif contribuer à protéger l'anonymat de l'utilisateur et rend plus difficile l'attribution de l'attaque.

Lors de l'opération Fancy Bear, en 2015, APT28 a distribué une application Android compromise sur des forums militaires ukrainiens[28]. L'application, avant d'avoir été comprise, avait été conçue pour aider au guidage des obusiers D-30 datant de l'époque soviétique et toujours utilisés par les Forces armées Ukrainiennes. Près de 9 000 militaires ont téléchargé l'application compromise, causant ainsi la mise hors-service d'un nombre considérable de canons – (jusqu'à 80 selon certaines estimations, démenties par Kiev)[29].

Modification des perceptions ou de la capacité d'analyse de l'adversaire

L'utilisation massive d'Internet comme source d'information au détriment des médias classiques (papier et télévision) crédibilise l'utilisation d'un botnet à des fins de manipulation de l'information, de propagande ou de désinformation. Par l'intermédiaire des bots, les machines infectées peuvent être paramétrées de sorte à télécharger du contenu faisant la promotion de certaines idées ou opinions, et le diffuser aux adresses courriels récupérées sur l'ordinateur compromis, relayer massivement des spams à un nombre important d'utilisateurs…

---

[25] Secrétariat général de la défense et la sécurité nationale, *Revue stratégique de cyberdéfense*, 12 février 2018, p. 15.
[26] « Hack attacks cut internet access in Liberia », *BBC News*, 4 novembre 2016.
[27] *Op. cit.* Koziel, Robinson, p. 24.
[28] Adam Meyers, « Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units », *Crowdstrike*, 22 décembre 2016.
[29] « Defense ministry denies reports of alleged artillery losses because of Russian hackers' break into software *», Interfax-Ukraine,* 06 janvier 2017.

En 2016, suite à l'exclusion des athlètes russes des Jeux olympiques de Rio, APT28 aurait infiltré les réseaux de l'Agence Mondiale Antidopage (AMA) et exfiltré puis publié en ligne des documents médicaux de sportifs américains, une façon de souligner et de rendre visible la différence de traitement accordé aux États-Unis et à la Russie.

On constate doncs ces dernières années une évolution dans l'utilisation des botnets : leurs usages sont plus variés et comprennent non seulement la destruction (DDoS) mais également les fuites de données et le espionnage. Leurs victimes sont également plus diversifiées. Au côté des ordinateurs s'ajoutent désormais les smartphones et l'IoT, comme l'a démontré l'opération Fancy Bear. Par conséquent, le nombre de vecteurs d'attaque (phishing, malware, etc.) a fortement augmenté.

Outil moderne au service d'opérations de renseignement, les botnets sont activement utilisés pour mener des attaques sophistiquées, comme l'illustrent les activités bien documentées d'APT28. L'un de leurs principaux intérêts est la difficulté à remonter jusqu'aux serveurs C&C et aux botmasters, ce qui demeure impossible dans de nombreux cas.

FOCUS INNOVATION

Storyzy : la classification de sources pour lutter contre la désinformation

La société

Fondée en 2012 par Arnaud Jacolin, Stanislas Motte, Ramón Ruti et Pierre-Albert Ruquier, issus des secteurs de la presse et des télécommunications, **Storyzy est une start-up indépendante** qui s'appuie sur une équipe de huit personnes, composée pour la moitié d'ingénieurs.

Constatant une dégradation de la qualité et de la fiabilité de l'information en ligne, **Storyzy** s'est spécialisée dans la détection de la désinformation en ligne, plus particulièrement la **classification de sites et chaînes vidéos de fake news**. La start-up propose à cet effet **une base de données de sources annotées** et **une plateforme SAS** (*Disinsformation Analysis Tool*) disponibles sous licence.

L'innovation

Utilisant le **traitement automatique des langues et le machine learning** (intelligence artificielle), la technologie de **Storyzy** permet d'**identifier et de catégoriser les sites internet et les chaînes vidéo qui pratiquent la manipulation de l'information sous 10 étiquettes** : haine, complotisme, extrémisme, propagande, désinformation, pseudoscience, satire, contenu viral et tabloïd.

Les données extraites des contenus des sources sont automatiquement analysées par les algorithmes développés par **Storyzy**. Ces derniers repèrent des similarités (citations, auteurs…) entre les sources déjà classifiées et les nouvelles puis attribuent un score à ces dernières. Selon ce dernier, les sources sont soit classées dans une ou plusieurs catégories de la désinformation, soit considérées comme fiables.

Les applications

Storyzy propose notamment trois services :

- Le ***Disinsformation Analysis Tool*** **(DAT)**, principalement mis à disposition des États et organisations (publicité, social media intelligence…). Plateforme web, le DAT analyse la relation entre la désinformation et les sources fiables. Ce moteur de recherche permet d'explorer l'écosystème de sources d'information qu'il classifie selon leur fiabilité éditoriale, ainsi que d'étudier la chronologie d'une propagation de fake news sur un sujet.
- **Une liste régulièrement mise à jour de sites internet pratiquant ou relayant la manipulation de l'information**, qui permet aux enseignes et commerces en lignes de sélectionner les sites sur lesquels ils souhaitent ou non voir figurer leurs bandeaux utilisés, et aux annonceurs publicitaires de se prononcer **contre le financement de la désinformation**.
- **News Coach**, un moteur de recherche qui compare les sites fiables et controversés, utilisé notamment à des fins de sensibilisation, mis à disposition des enseignants et éducateurs afin de les aider à développer l'esprit critique des jeunes face à la désinformation.

L'actualité

Initialement destinés à vérifier l'origine des information économique et financière, les outils de Storyzy ont progressivement été étendus aux enjeux de la manipulation de l'information.

En partenariat avec le ministère des Armées depuis 2015, Storyzy s'est ensuite intéressée à la **détection de l'omission de l'information** et à la **contre-argumentation face à la désinformation**. La start-up a d'ailleurs bénéficié de financements de la Direction générale à l'Armement via deux programmes Rapid.

Storyzy interviendra le 16 octobre lors d'un petit déjeuner thématique, organisé conjointement par CEIS et le Commandement de la cyberdéfense du ministère des Armées, sur les "**Deepfakes : armes de guerre de la désinformation**" au CEIS Lab (40 rue d'Oradour sur Glane, 75015 Paris).

CALENDRIER

27/11 : Cyberdéfense et entreprises

Innovation, cyberdéfense et OpenDATA

La seconde édition de l'événement **Cyberdéfense et entreprises**, organisé par CEIS au profit du Commandement de la cyberdéfense, aura lieu le 27 novembre 2019 sur la thématique « **Innovation, cyberdéfense et OpenDATA** ».

Cet événement s'inscrit dans la suite de l'inauguration le 03 octobre par la ministre des Armées de la **Cyberdéfense factory**, premier incubateur au service des opérationnels de la cyberdéfense, à Rennes. Projet piloté et financé par le Commandement de la cyberdéfense et la Direction générale de l'Armement, la Cyberdéfense factory a pour objectif de rapprocher la recherche, les entrepreneurs et les opérationnels afin de faciliter le développement et l'acquisition de produits et services innovants en matière de cyberdéfense.

ACTUALITÉ

La France rappelle sa position en faveur de l'application du droit international au cyberespace

Alors que les négociations internationales sur les enjeux de cybersécurité reprennent à l'ONU, d'abord au sein de l'Open Ended Working Group, puis dans le cadre Groupe d'Expert Gouvernemental ensuite, la France rappelle sa position sur l'applicabilité du droit international aux opérations dans le cyberespace, en temps de paix comme de guerre. À l'inverse de nombreux autres acteurs, qui adoptent sur cette question un positionnement parfois ambigu, la France témoigne ainsi de son exemplarité et de sa transparence sur ce sujet.

Dans un rapport de septembre 2019 porté par le Commandement de la cyberdéfense, la Direction des affaires juridiques et la Direction générale des relations internationales et de la stratégie, la ministre des Armées réitère l'engagement de la France pour promouvoir la coopération internationale dans le cyberespace. Ce document a ainsi vocation à :

- Nourrir les réflexions du GGE, dont les membres se réuniront à l'ONU d'ici la fin de l'année 2019 pour un nouveau cycle de négociation, après les résultats mitigés du dernier round en 2017.
- Rappeler la position de la France en faveur de l'applicabilité du droit international, incarné par la Charte des Nations unies et le droit international humanitaire, au cyberespace et aux technologies de l'information et de la communication, en temps de paix comme en temps de guerre.

- Contribuer à promouvoir un cyberespace pacifique et sûr, et ce notamment en réduisant les risques d'incompréhension ou d'escalade non maîtriséedans cet environnement.

Ce rapport s'inscrit dans le prolongement des réflexions et travaux du ministère des Armées visant à préparer la France aux conflits du XXème siècle, concrétisés d'une part par la Stratégie nationale de cyberdéfense de février 2018, et d'autre part par la Doctrine en lutte informatique offensive de janvier 2019.

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 des Armées
Direction Générale des Relations Internationales et de la Stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com