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

Table des matières

ANALYSES

1. LE PARADOXE TOR

Lancé en 2001, Tor est le plus connu des « darknets », ces réseaux superposés, ou overlay qui, à l'instar de I2P ou de Freenet, se superposent aux réseaux existants avec des applications et une couche de protocoles proposant des fonctionnalités d'échange de fichiers et un écosystème complet (sites, blog, mail, chat…) offrant un fort niveau d'anonymisation. Utilisant des technologies de routage « en oignon » développées par l'US Navy dans les années 90, largement financé par le Gouvernement américain pour promouvoir la démocratie dans le monde, refuge pour cybercriminels en tout genre, Tor est en même temps soutenu par la plupart des organisations de défense de la vie privée au nom de la liberté d'expression et de la lutte contre « big brother ». C'est là tout le paradoxe de ce réseau qui est aujourd'hui à la croisée des chemins et cherche à gagner en respectabilité. Il devrait d'ailleurs prochainement être intégré directement dans Firefox pour offrir un mode de navigation « super privé ».

Qu'est-ce que TOR ?

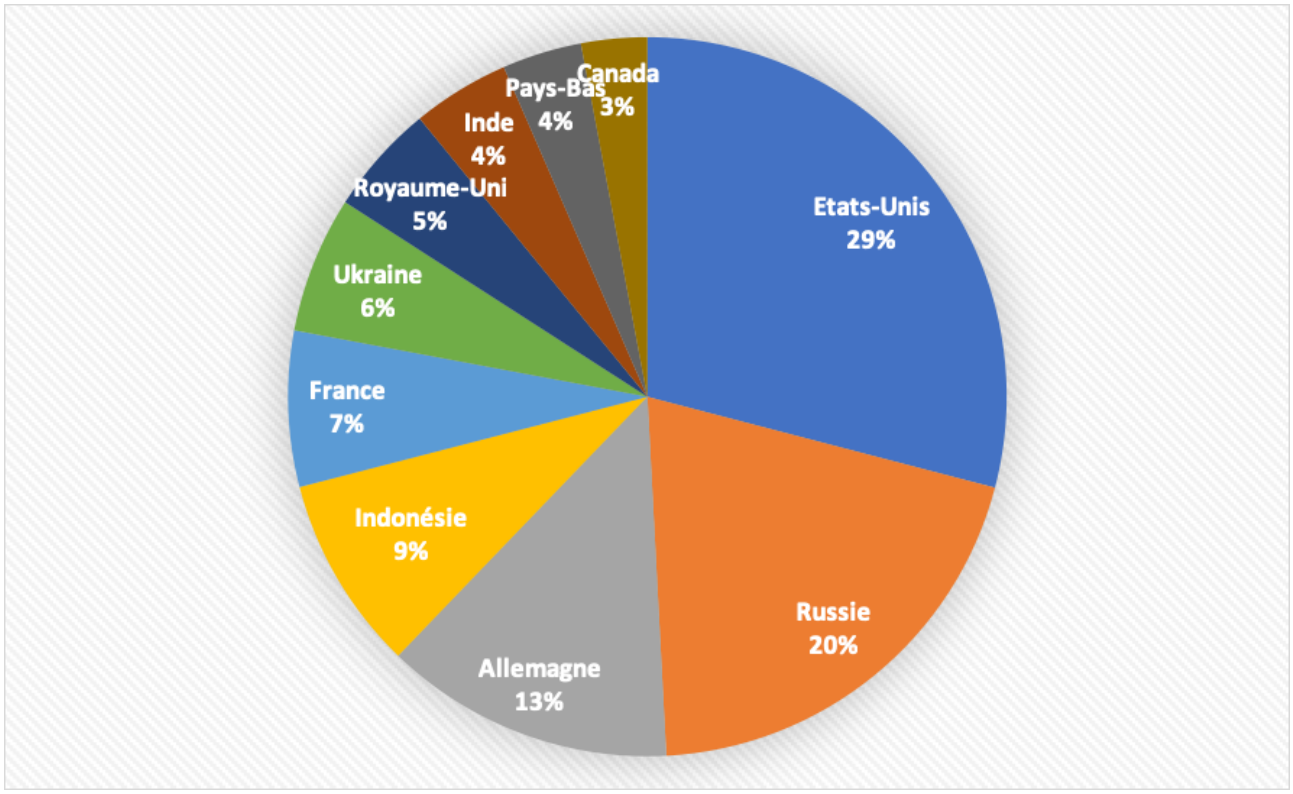
Créé aux USA dans les années 1990 par le US Naval Research Laboratory, Tor est à l'origine un projet militaire qui avait pour objectif de permettre aux communications de la Défense de se fondre dans l'anonymat du réseau et de gagner en résilience.

En pratique, Tor recouvre principalement 2 choses :

- Des fonctionnalités de connexion sécurisées permettant de naviguer de façon anonyme sur internet. Le navigateur Tor permet de se connecter à une cible via une série de relais qui assurent un routage « en oignon » en utilisant des canaux de communications chiffrés, ce qui assure à l'internaute un haut niveau d'anonymat. Tor se caractérise donc par une architecture maillée comprenant environ 7 000 relais. Parmi les fonctionnalités proposées : SecureDrop(1), lancé en 2013, qui permet les échanges sécurisés entre journalistes et sources d'information, et qui a été adopté par le New York Times ou le Washington Post ;
- Des blogs, sites, forums, et places de marché. On y dénombre notamment entre 45 et 60 000 « Hidden Services » (ou HSE) qui sont en forte progression (2). Accessible uniquement via des annuaires d'adresses et quelques moteurs spécialisés, ils représentent moins de 8% du trafic total du réseau Tor mais rassemblent une population d'environ 600 000 utilisateurs actifs. A noter qu'à côté des HSE, certaines ressources sont désormais ouvertes. Depuis 2014, Facebook a ainsi créé son propre site dans Tor afin de protéger ses utilisateurs de la censure en place dans certains pays. Selon les chiffres communiqués par l'entreprise, un million d'individus se connecteraient aujourd'hui au réseau social via Tor.

Au total, Tor représente un volume total de 2,5 millions d'utilisateurs par jour pour l'ensemble de ses services. Au plan géographique, Etats-Unis et Russie arrivent en tête, la France arrivant en 5ème position avec environ 125 000 utilisateurs réguliers.

Top 10 des pays utilisateurs de TOR



Source : https://metrics.torproject.org/userstats-relay-table.html

Les « Hidden services » montrés du doigt

Ce n'est donc pas tant Tor en général que les HSE en particulier qui soulèvent aujourd'hui un véritable défi de sécurité et d'ordre public(3). Compte tenu de l'anonymat quasi absolu qu'il procure à ses utilisateurs, le réseau est en effet devenu :

- Un accélérateur de la criminalité traditionnelle (pédopornographie ; trafic de drogue, d'armes, de biens volés, de contrefaçons, de numéros de cartes bancaires ; piratage d'œuvres audio-visuelles…). La pédopornographie représenterait même, selon une étude de l'Université de Porstmouth, 80% des consultations(4). Une dérive reconnue par Andrew Lewman, ancien directeur du Tor Project jusqu'en 2015 et aujourd'hui à la tête de la société Owl Cybersecurity, spécialisée dans « l'intelligence » sur le darkweb, quand il admettait récemment que 95% de l'activité de Tor était devenue criminelle…(5) ;
- Un élément clé de la « kill chain » cybercriminelle, via la mise à disposition de ressources permettant la réalisation d'attaques informatiques (vente d'identifiants et de mots de passe volées, de services d'attaque « as a service » …) ou la commercialisation des données volées lors d'une attaque. Il semble d'ailleurs que le réseau Tor et ses HSE soient de plus en plus utilisés dans le cadre d'attaques DDoS ou APT. Un rôle également facilité par l'explosion des crypto-monnaies et notamment du Bitcoin dont l'utilisation en tant que moyen de paiement sur les Darknets aurait atteint 603 millions de dollars en 2018 après un record à 707 millions en 2017(6).

Certaines organisations terroristes, notamment islamistes, ont enfin pris conscience du potentiel des darknets pour échanger, préparer et financer des opérations ou bien encore mener des campagnes de propagande, comme en témoigne le guide publié en 2015 par l'Etat islamique(7). Même s'il comportait un certain nombre de conseils très basiques et quelque peu déconnectés des réalités, l'ouvrage témoignait aussi de l'intérêt que pouvait susciter les Darknets pour des organisations terroristes.

Qui gère et finance Tor ?

Le *Tor project* est depuis 2006 géré par une organisation à but non lucratif(8), qui en assure la maintenance pour un budget d'environ 3 à 4 millions de dollars par an avec le soutien de nombreux lobbies militant pour la protection de la vie privée et contre la surveillance de masse, comme l'Electronic Frontier Foundation (EFF) ou l'American Civil Liberties Union (ACLU). Dans le même temps le projet était financé en quasi-totalité jusqu'en 2017 par le gouvernement américain via l'US Navy, le State Department, ou bien encore le Broadcast Board of Governors, émanation de la CIA assurant la diffusion de contenus audio-vidéo à l'étranger, notamment à travers des radios comme Radio Free Asia ou Radio Free Europe.

Un rapport publié par le Tor project indique ainsi que 85% de ses ressources provenaient du gouvernement américain en 2015, 76% en 2016, 51% en 2017(9). L'organisation lorgne désormais sur des financements privés (Mozilla, Reddit, Duckduckgo…) pour diminuer sa dépendance aux fonds publics et restaurer sa réputation, largement entachée par les révélations concernant ses liens étroits avec le gouvernement américain. *« Tor est devenu une « extension privée » du gouvernement qu'il prétendait combattre »*, souligne le journaliste Yasha Levine(10) qui a exploité de nombreux documents communiqués au nom du Freedom of Information Act.
De fait, l'organisation doit faire oublier quelques épisodes fâcheux, à commencer par les révélations d'Edward Snowden en 2013 sur l'existence du programme Bullrun visant notamment à « désanonymiser » le réseau, ou, plus récemment, celles concernant le « hacking » du réseau par l'Université Carnegie Mellon, à la demande du FBI, dans le cadre des investigations sur le site Silk Road(11). *« En réalité, depuis l'affaire Snowden, le statu quo en ce qui concerne Tor semble n'avoir pas bougé : la NSA ou le GCHQ, comme d'autres grandes agences de renseignement COMINT, sont tout à fait capables de désanonymiser un ou plusieurs utilisateurs de TOR en utilisant de différentes techniques, mais il reste pour le moment apparemment impossible de le faire à grande échelle pour rendre le trafic de Tor accessible. Et accéder au trafic d'autres réseaux tels que Freenet ou I2P est aussi compliqué, voire plus difficile »* souligne Laurent Gayard dans un récent ouvrage très complet sur le sujet(12). De fait, les tentatives, réussies ou pas, de l'Administration américaine pour obtenir des données sur les utilisateurs et les contenus de Tor ont au moins eu le mérite d'attester qu'il n'existait pas de « backdoor » par défaut dans le système…

Comment réguler les Darknets ?

Le premier moyen est l'auto-régulation. Celle-ci existe bel et bien sur certains blacks markets, les utilisateurs se liguant contre les personnes ne respectant pas les « codes éthiques » établis, notamment celles qui se livrent à l'apologie du terrorisme ou à l'échange de contenus pédopornographiques. La sanction peut aller jusqu'au bannissement de l'utilisateur ou au « dox », c'est-à-dire la révélation au public des données le concernant. Fondée sur l'éthique « à géométrie variable » des utilisateurs des darknets, cette auto-régulation est bien évidemment insuffisante…

Pour que Tor n'échappe pas totalement à ses créateurs et ne soit pas une zone de non-droit, il faut donc envisager différentes capacités techniques, comme le soulignaient en 2015 Michael Chertoff et Tobby Simon, pour la Global Commission on Internet Governance(13) :

- La cartographie des « hidden services » (HSE) grâce au déploiement d'un nœud permettant d'exploiter la base de données distribuée utilisée pour la résolution des domaines. La possibilité de déployer pour tout un chacun un nœud de sortie est en effet l'un des points faibles du réseau ;
- La surveillance des HSE par des acteurs publics et privés. La tâche est particulièrement difficile compte tenu de leur volatilité : 90% d'entre eux se renouvèlent tous les 18 mois. La DARPA finance à cet égard plusieurs projets comme Memex(14), tandis qu'en France une société comme Aleph Networks(15) collecte et indexe désormais des millions de pages sur Tor ;
- La surveillance des « paste bin » et autres ressources du « deep web » qui constituent souvent des portes d'entrée vers les darknets et qui permettent de cibler des domaines Tor à surveiller ;
- L'exploitation des données des fournisseurs d'accès pour identifier les connexions à des domaines « non standard » ;
- La surveillance des transactions financières opérées depuis le darkweb. Contrairement aux idées reçues, les flux Bitcoin ne sont pas anonymisés mais pseudonomysés. Ils sont donc traçables.

Autant de capacités qui sont le préalable indispensable à toute judiciarisation des affaires concernant les Darknets. C'est ainsi que le FBI a pu fermer Silk Road en 2013 ou bien encore mener conjointement avec Europol l'opération Onymous en 2014 pour fermer 400 sites vendant de la drogue et des armes. Autre exemple plus récent : la fermeture du marché noir francophone Black Hand en juin 2018 qui comptait 3 000 inscrits(16).

La lutte contre les dérives des Darknets procède donc d'une course de vitesse permanente entre les criminels et les autorités, avec le risque que ne se développe des Darknets encore plus « sombres », et donc encore plus compliqués à réguler, au fur à mesure que Tor gagne en respectabilité.

[1] https://securedrop.org/

[2] A comparer aux 2 milliards de sites web.

[3] Lire à ce propos la note stratégique de CEIS sur les Black Markets francophones accessible sur : https://ceis.eu/wp-content/uploads/2019/01/NoteStrat_Black_Market_Web.pdf

[4] https://www.theguardian.com/technology/2014/dec/31/dark-web-traffic-child-abuse-sites

[5] https://www.cyberscoop.com/tor-dark-web-andrew-lewman-securedrop/

[6] https://blog.chainalysis.com/reports/decoding-darknet-markets

[7] https://www.centerforsecuritypolicy.org/2015/05/20/islamic-state-supporters-publish-a-how-to-guide/

[8] https://www.torproject.org/about/overview.html.en

[9] https://blog.torproject.org/transparency-openness-and-our-2016-and-2017-financials

[10] https://surveillancevalley.com/blog/fact-checking-the-tor-projects-government-ties

[11] https://www.zdnet.fr/actualites/desanonymisation-de-tor-carnegie-mellon-etait-effectivement-impliquee-39833322.htm

[12] Géopolitique du Darknet, nouvelles frontières et nouveaux usages du numérique, ISTE Editions, janvier 2018.

[13] https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf

[14] https://www.usine-digitale.fr/article/la-darpa-cree-le-google-du-dark-web-pour-aider-la-police-dans-ses-enquetes-sur-les-trafics-en-tout-genre.N312950

[15] http://www.aleph-networks.com/

[16] https://www.nextinpact.com/brief/arrestations-en-serie-pour-des-pirates-de-l-internet-clandestin–black-hand-et-rex-mundi-4439.htm

2. L'IRAN ET L'ARME CYBER : ENTRE DIPLOMATIE ET DESTABILISATION

Depuis la fin des années 2000, l'Iran a régulièrement été accusé d'avoir orchestré des cyberattaques contre certains de ses rivaux, notamment les Etats-Unis et l'Arabie Saoudite. La montée en capacités cyber du pays s'inscrit dans un contexte international tendu, marqué d'abord par la rivalité entre l'Iran et l'Arabie saoudite, tous deux impliqués dans les conflits régionaux, et ensuite par le régime de sanctions imposées à l'Iran par les Etats-Unis en réaction au programme nucléaire iranien.

Le choix par l'Iran de l'arme cyber pour répondre à des menaces extérieures s'explique aussi par un évènement particulier : le choc constitué par l'attaque Stuxnet, menée par les États-Unis avec le soutien d'Israël entre 2009 et 2011. Projet de l'administration Bush prolongée par l'administration Obama, l'attaque avait visé les installations nucléaires iraniennes de Natanz et avait provoqué la destruction d'un millier de centrifugeuses. Cette atteinte à ses infrastructures vitales a poussé l'Iran à développer un système de cyberdéfense, à renforcer ses capacités dans ce domaine, et à mettre en œuvre des cyberattaques, qu'elles soient ou non commanditées par le régime.

La période d'accalmie qui semblait s'être installée avec la mise en place de l'accord sur le nucléaire iranien (Joint Plan of Action, JCPOA) pourrait trouver son terme avec le retrait des États-Unis de cet accord. Ce positionnement ravive en effet les craintes de cyberattaques iraniennes contre les Etats-Unis ou même l'Europe, si cette dernière ne réussissait pas à préserver ses engagements dans le cadre du JCPOA.

Les cyberattaques : armes de déstabilisation dans les rivalités régionales

Les cyberattaques attribuées à l'Iran sont de natures diverses et répondent à différentes logiques. Qu'elles visent le vol ou la destruction de donnée, ou encore l'espionnage, elles s'inscrivent dans un contexte géopolitique particulier et répondent à des objectifs précis.

Des cyberattaques importantes ayant visé en priorité l'Arabie Saoudite et plus largement le Moyen-Orient, impliquant le vol ou la destruction massive de données, ont régulièrement été imputées à l'Iran depuis le début des années 2010. Le contexte géopolitique régional et international permet d'éclairer les objectifs de certaines attaques. Ainsi, la première attaque de grande envergure menée contre certains pays du Golfe, nommée Shamoon par les experts de la société Symantec, avait sans doute un double objectif : contenir l'intervention des pays ciblés sur le dossier nucléaire iranien discuté au plan international et mettre à mal leurs principales ressources économiques. En 2012, Shamoon a d'abord visé la société Aramco, leader du pétrole saoudien. L'attaque avait été annoncée et revendiquée sur Pastebin par le groupe de pirate informatique Cutting Sword of Justice, considéré à ce jour comme responsable de l'attaque. Dans son annonce, le groupe reprochait à l'Arabie Saoudite son intervention dans les guerres du Moyen-Orient et son soutien au « terrorisme islamiste sunnite mondialisé », ainsi que son ingérence dans les affaires iraniennes. L'Arabie Saoudite avait en effet déclaré quelques mois plus tôt qu'elle était prête à compenser par sa propre production de pétrole la diminution à venir de celle de l'Iran résultant du régime de sanctions. Au total, plus de 30 000 ordinateurs de la société Aramco ont été endommagés, provoquant des fuites de données massives et des pertes financières considérables dont les montant exacts n'ont pas été publiés. La société Qatari RasGas a ensuite été touchée par un malware très similaire peu de temps après. Une version améliorée du malware, Shamoon 2, a touchée

en 2016 et 2017 plusieurs sociétés du Golfe, dont le nombre et les identité précises, ainsi que l'étendue des dommages, sont difficiles à recueillir.

L'arme cyber, levier d'influence sur la scène internationale.

Certaines des attaques imputées à l'Iran ont également pu avoir pour objet de faire pression sur les États-Unis lors des négociations de l'accord sur le nucléaire iranien. Ainsi, l'opération Ababil consistait en une attaque de type Distributed Deny of Service (DDoS) visant de nombreuses institutions bancaires américaines entre 2011 et 2013, empêchant des dizaines de milliers de clients d'accéder à leurs comptes bancaires. De même en 2014, la société Las Vegas Sand Corporation a vu plusieurs milliers de serveurs et ordinateurs endommagés par un malware, au cours d'une attaque sans doute menée en réaction aux propos de son fondateur, proposant de bombarder l'Iran pour le forcer à abandonner son programme nucléaire. Ces deux exemples de représailles mettent bien en lumière les moyens d'expression et de pression dont l'Iran peut faire usage afin de réaffirmer ses positions et son influence. D'autres opérations plus simples impliquaient le défacement de sites Internet américains. Il s'agissait sans doute là aussi pour l'Iran de démontrer leur capacité de nuisance dans l'éventualité de l'échec de la mise place d'un accord. Il est d'ailleurs intéressant de noter que dans l'ensemble, ces opérations ont rapidement pris fin lors de la mise en place du JCPOA.

Au-delà de la date à laquelle ces attaques ont été menées, la temporalité de leur révélation est elle-même un outil diplomatique s'insérant dans un agenda politique précis. Par exemple, suite à l'accalmie des deux premières années qui ont suivi la signature de l'accord sur le nucléaire, les accusations américaines contre l'Iran ont repris suite aux prises de fonction de Donald Trump, qui affichait déjà pendant sa campagne présidentielle sa volonté de remettre en cause le JCPOA. Au printemps 2016, quelques mois avant l'élection présidentielle américaine, deux sociétés iraniennes et certains de leurs employés ont ainsi été accusés par la justice américaine d'avoir participé à l'opération Ababil en 2011-2013. Toujours en 2016, deux iraniens avaient aussi été accusés du vol, entre 2007 et 2014, de logiciels de la société ArrowTech permettant le développement de missiles. Pour tous ces cas, les tribunaux américains avaient déterminé et rendue publique l'identité des individus – iraniens, présumés responsables les attaques. Les accusations américaines se sont multipliées en 2017 et 2018, concernant entre autres incidents :

- Une opération de vol de données ayant débuté en 2013 et ayant principalement touché des universités ;
- Un ransomware exigeant 6 millions de dollars de la chaîne américaine de télévision HBO, symbole de la culture et de l'industrie cinématographique américaine. Dans le même domaine, des épisodes de la fameuse séries *Game of Thrones* ont également fuité. Le piratage et la revente de logiciels d'armement américains à la société ArrowTech Associates.
- Le piratage des e-mails de près de trente parlementaires britanniques. Les suspicions britanniques s'étaient d'abord portées sur la Russie, avant d'être redirigées quelques mois plus tard vers l'Iran.
- En 2018, une opération ayant débuté en 2015 et visant notamment des hôpitaux et structures du domaine de la santé américains aurait permis, avec l'usage d'un ransomware, d'extorquer auprès de près de 200 victimes plus de 6 millions de dollars

Notons que si la réalité de la plupart de attaques n'est pas à mettre en cause, toutes n'ont pas pu être attribuées à l'Iran avec certitude, c'est-à-dire qu'il n'a pas été possible d'établir de façon irréfutable qu'elles ont été menées par des acteurs iraniens ou qu'elles ont été commanditées par le régime. A titre d'exemple,

les rapports publiés par la société FireEye concernant les attaques de type *Advanced Persistant Threat* (APT), mentionnent presque toujours un « responsable présumé ». En effet, dans le cas de l'Iran, la présence d'éléments de langage en persan, ou d'adresses e-mails appartenant à des iraniens dans certains des codes, peut n'être que le résultat d'une manipulation des auteurs réels de l'attaque.

De la même façon, aucun rapport n'a confirmé l'annonce faite par les autorités iraniennes en novembre 2018, qu'une attaque de type Stuxnet 2.0 avait été contenue par leurs services chargés de la cyberdéfense. Ces derniers ont rendu les États-Unis et Israël responsables de cette attaque qui aurait ciblée les infrastructures de télécommunication du pays. Quelques jours plus tôt, des responsables avait par ailleurs fait part de la mise sur écoute de téléphones de hauts responsables iraniens, dont le Président Hassan Rohani.

Conclusion

Comme le montre l'exemple iranien, l'utilisation de l'arme cyber, tout comme la revendication, la révélation, et l'attribution des cyber-attaques, participe donc profondément d'une logique de représentation et de pression diplomatique sur la scène régionale et internationale, au-delà d'un simple moyen d'affaiblir matériellement ses opposants. Dans le cas iranien, les attaques dont l'Ian a été accusé d'être responsable, ou que le régime a annoncé avoir subies, replacent l'Iran, même de façon involontaire, sur le devant de la scène internationale comme l'auteur d'attaques menées contre l'Occident ou la victime de d'attaques menées à son encontre, et participant d'une escalade des tensions et d'une déstabilisation des relations avec l'Europe en particulier.

FOCUS INNOVATION

QUANTCUBE TECHNOLOGY : EXPLOITER LES DONNEES ALTERNATIVES

Présentation

Quantcube Technology a été créée en 2013. Cette start-up française issue de la FinTech est spécialisée dans l'exploitation des données « alternatives ». Son expertise algorithmique lui permet de transformer des données massives (*Big Data*), hétérogènes et non structurées en prévisions politiques, économiques et financières ultra-précises.

L'innovation

QUANTCUBE exploite des données « alternatives », c'est-à-dire à la fois :

- les données générées par les individus : réseaux sociaux, blogs, *consumer reviews*, réseaux professionnels, etc.
- les *open data*, données produites par les entités publiques : données gouvernementales, données publiques des entreprises, données commerciales, etc.
- les données générées par des machines : images satellites, trafic aérien et maritime, données météorologiques, etc.

Il s'agit de données brutes, que Quantcube Technology agrège et analyse afin d'obtenir des prévisions macroéconomiques en temps réel. Pour cela, la start-up utilise des technologies *Big Data* (Spark ou Hoop par exemple), ainsi que des algorithmes d'intelligence artificielle développés en interne. Ses équipes de *data scientists* multilingues (français, anglais, arabe, russe, chinois, etc.), sont spécialisées à la fois dans le traitement automatique du langage (analyse de textes), le *deep learning* (reconnaissance d'images) et les algorithmes de graphes (corrélations entre différents acteurs). Le niveau de corrélation par rapport aux chiffres officiels atteint 85 à 95%, avec un à six mois d'avance.

Un des produits phares de Quantcube Technology est la plateforme de prévisions en temps réel « *Global Macro Smart Data* », commercialisée sous la forme d'une licence annuelle. A titre d'exemple, depuis mai 2013, Quantcube Technology a atteint un taux de précision de 92% pour la prédiction des résultats de 21 élections politiques, et ce plusieurs semaines avant les événements en question. La start-up a notamment prédit les résultats du référendum pour le Brexit (2016), l'élection de Donald Trump en 2016 (avec quinze jours d'avance), les résultats du premier tour des élections présidentielles françaises de 2017, ainsi que l'issue des *mid-term* américaines de 2018. L'outil peut également évaluer le potentiel de croissance d'une ville, d'une région ou d'un pays et mesurer son niveau d'instabilité sociale, voire la probabilité d'une crise. Les algorithmes de Quantcube Technology offrent aussi la possibilité de détecter des anomalies dans différents flux, tels que le trafic aérien ou maritime ou encore les échanges commerciaux entre plusieurs entités ou États.

Les serveurs développés en interne par Quantcube Technology sont capables de traiter près d'un million d'images en simultanés avec un haut niveau de précision : les algorithmes sont capables d'identifier des éléments spécifiques (immeubles, ponts, routes, champs, ruisseaux, véhicules, etc.) mais également de les classer par catégories (écoles, hôpitaux, habitations, voiture, moto, etc.) grâce à une granularité de plus en plus fine.

Les usages

La technologie de Quantcube Technology permet un certain nombre d'usages intéressants pour la défense, notamment dans le cadre du renforcement des fonctions « connaissance et anticipation », mis en avant dans la Loi de programmation militaire (LPM) 2019-2025. En effet, accentuer la connaissance et l'anticipation permet de mieux comprendre les causes et les conséquences d'une crise, ainsi que d'apporter des réponses adaptées à leur résolution.

♣ Analyse des signaux faibles/détection d'anomalies dans tous les domaines liés à la défense : tendances économiques, politiques, évolution du marché de l'armement, etc.

♣ Anticipation des crises ou des ruptures potentielles

♣ Analyse de flux afin de détecter des réseaux criminels ou de surveiller l'activités de certains groupes

♣ Identification d'infrastructures/de sites militaires en zones à risque afin de connaître leur configuration et de surveiller les flux qui les caractérisent

♣ Contextualisation des données brutes traitées par les algorithmes de Quantcube Technology grâce à l'agrégation de données militaires

La connaissance d'une zone, d'un pays, d'un marché ou de flux, ainsi que l'anticipation d'une crise ou d'une anomalie permet notamment aux autorités publiques militaires de conserver la supériorité informationnelle dans les opérations.

CALENDRIER

Le Paris Region Cybersecurity Challenge

La Région Île-de-France, en partenariat avec Systematic Paris-Region, Hexatrust et le CEA LIST, organisent pour la première fois le Paris Region Cybersecurity Challenge.

Des start-ups, TPE/PME ou ETI seront mises au défi de répondre à des besoins précis en matière de cybersécurité exprimés par des acteurs économiques franciliens.

Trois thématiques ont été retenues pour l'édition 2019 :

- L'événementiel (défi porté par Atos) : Comment renforcer la sécurisation d'événements majeurs dans l'espace public ?
- Les transports (défi porté par la SNCF) : Comment garantir la protection des données des voyageurs qui sont échangées entre transporteurs, collectivités et autres acteurs ?
- Le sport (défi porté par le Stade de France) : Comment développer des applications permettant d'optimiser le « parcours client » en faisant interagir les données de plusieurs acteurs (opérateurs de transports en commun, gestionnaires d'infrastructures routières…) ?

Les trois projets les plus intéressants pour chaque défi seront proposés aux élus régionaux et subventionnés à hauteur d'1 million d'euros au total.

Inscriptions sur le site dédié avant le 25 février 2019 à 23h59.

Intervention de Florence Parly, ministre des Armées, Forum international de la Cybersécurité

Lors de son intervention en ouverture de la plénière dédiée à l'autonomie stratégique le 22 janvier 2019, la ministre des Armées a rappelé la gravité de la menace cyber, et la nécessité d'une cybersécurité « by design » pour y faire face. Dans le prolongement de son discours du 18 janvier, elle a fait les annonces et pris les engagements suivants :

- Elle a d'abord donné quelques chiffres, précisant qu'en 2017, les réseaux de la défense avaient subi 700 événements de sécurité dont 100 cyberattaques, un chiffre qui a progressé pour s'établir à 700 en 2018.
- Elle a réaffirmé la mise en place d'une doctrine offensive en matière de cyberdéfense reposant sur la lutte informative offensive, réaffirmant que l'arme cyber était déjà utilisée en opération et insistant sur la nécessité de l'intégrer à tous les programme d'armement.
- Elle rappelé son engagement en faveur d'une plus grande coopération avec les partenaires européens du ministère des Armées, en vue de l'émergence d'une culture commune, et de la mise en place dispositifs communs de protection.
- Elle a proposé aux industriels de défense une collaboration renforcée pour la protection de la chaîne d'approvisionnement, qui devra passer, d'ici l'été, par la formulation avec l'ANSSI d'engagements mutuels en matière de cybersécurité dans le but de protéger le développement, la fabrication et la maintenance des équipements de défense.
- Elle a annoncé l'établissement d'un partenariat entre le Commandement de la Cyberdéfense et la start-up française YesWeHack, plateforme de bug bounty qui permettra au ministère des Armées de lancer, en février 2019, son premier « bug bounty » réalisés par des hackers éthiques recrutés au sein de la réserve opérationnelle cyber.
- Plus largement, elle a rappelé son engagement aux côtés des PME et le lancement du Plan Action PME et de ses 40 mesures destinées à mieux prendre en compte les PME dans la stratégie d'achat du ministère des Armées et à rééquilibrer la relation avec les grands groupes.

Elle a enfin appelé tous les acteurs de la cybersécurité à agir de concert pour assurer la cyberdéfense de la France et de l'Europe.

Retrouvez l'intégralité de son discours sur le site du FIC2019, et son intervention en image ICI.

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