Lettre mensuelle – **Mars 2021** – **Disponible sur omc.ceis.eu**

Table des matières

ANALYSES (1/2)

UN PLAFOND DE VERRE POUR LE STOCKAGE DE DONNÉES ?

La convergence du web 2.0, des services Cloud et du Big Data a démultiplié les besoins en stockage de données. À cette convergence s'ajoutent le développement de l'IoT et la connectivité grandissante dans les pays en développement (on passerait ainsi de 5 milliards de personnes connectées en 2019 à 6 milliards en 2025[1]), qui ne font que renforcer cette tendance. Selon l'Académie des Technologies, la sphère globale des données (SGD) augmenterait d'un facteur d'environ mille tous les vingt ans[2] rendant l'approche actuelle de stockage de données insoutenable au-delà de 2040.

Les armées et le secteur de la défense en général ne font pas exception et présentent également de forts besoins en matière d'hébergement de données. Ces besoins concernent aussi bien les données exploitées de façon directe en opération, que celles qui le sont dans le cadre de projet d'analyse de données massives. La création de la DGNum en 2018, qui s'inscrit notamment dans un objectif de capitalisation de la donnée, reflète et accentue l'explosion de ces besoins de stockage de données au sein des armées. Les données suivantes sont particulièrement stratégiques pour la défense :

- Les données de santé, dont on estime pour le secteur civil que le volume double tous les 73 jours[3] ;
- Les données issues du renseignement et notamment du SIGINT, OSINT et GEOINT. A ce titre, les données vidéos représentent une part très importante des besoins (données capturées par satellites, drones, etc.) ;
- Les données utilisées dans le cadre de la R&D, par exemple pour l'entraînement de réseaux neuronaux.

La problématique de soutenabilité de ce stockage est liée à plusieurs facteurs :

- Un coût énergétique, auquel on pourrait associer l'énergie nécessaire à l'exploitation des données ;
- Un coût lié à l'espace occupé par les datacenters hébergeant ces données ;
- Un coût environnemental, de plus en plus pris en compte par les Etats dont les politiques en la matière pourraient entraîner une répercussion de ces coûts sur l'industrie sous forme de taxe.

D'autre part, les besoins en typologie de stockage évoluent. Le développement du Big Data nécessite que de grandes quantités de données soient stockées sous une forme accessible à des fins de traitement : les besoins en stockage de vastes volumes de données correspondent ainsi de moins en moins à un stockage de données "à froid" privilégié pour l'archivage, et de plus en plus à un stockage "à chaud", laissant les données accessibles en ligne pour traitement permettant d'en extraire de la valeur. L'enjeu n'est donc pas qu'une question de volume, mais également de performances liées au support de stockage.

Dans ce contexte, l'équilibre entre la valeur de la donnée et le coût de son stockage rend d'autant plus urgents les progrès dans ce domaine. Une demande en capacité de stockage bien supérieure à l'offre influerait défavorablement sur le coût du stockage, limitant la marge de manœuvre du propriétaire des données : celui-

[1] https://www.seagate.com/fr/fr/our-story/data-age-2025/

[2] https://www.academie-technologies.fr/blog/categories/publications-de-l-academie/posts/archiver-les-megadonnees-au-dela-de-2040-la-piste-de-l-adn

[3] https://www.dsih.fr/article/4134/doublement-du-volume-des-donnees-d-e-sante-tous-les-73-jours.html

ci devra alors faire le choix de réduire la quantité ou la qualité des données afin d'en réduire le volume. Dans le secteur de la défense, cela pourrait se traduire à budget égal par une diminution de l'efficacité de la R&D et des capacités opérationnelles des armées.

Pour faire face aux problématiques de croissance des besoins de stockage de données, faut-il se résigner à une certaine frugalité dans les usages ou peut-on espérer le salut sous forme technologique ?

1. Technologies actuelles

Il existe trois principales formes traditionnelles de stockage de masse des données :

- Le **stockage magnétique**. Aujourd'hui, il concerne principalement les disques durs (en anglais *Hard Disk Drive* ou HDD) et le stockage sur bande pour l'archivage. Les disques durs sont constitués de plateaux recouverts d'une surface magnétique et parcourus par des têtes de lecture et d'écriture (cette technologie implique donc des interactions mécaniques). La donnée est inscrite par modification de la polarité des particules magnétiques à la surface du disque.

Vue interne d'un disque dur contenant 3 plateaux superposés – Source : Wikipedia

De leur côté, les bandes magnétiques destinées à la sauvegarde se présentent sous la forme de cartouches contenant une bande enroulée. Cette technologie représentait le standard du stockage de données depuis les années 50, mais leurs caractéristiques inhérentes les ont peu à peu reléguées au seul archivage de données. Plus spécifiquement, le mode de lecture purement séquentiel des données implique que l'on ne peut pas accéder rapidement à des données situées à différents endroits du support. Pour autant, cette technologie reste parfaitement d'actualité pour cet usage d'archivage : notons ainsi que les GAFA, que l'on peut difficilement soupçonner d'être à la traîne en matière d'usage de solution innovantes, sont aujourd'hui les premiers consommateurs de bandes magnétiques[4].

[4] https://www.cfigroupe.com/medias/pdf/guide-pratique-ibm-cfi-final.pdf

Vue interne d'une cartouche LTO-2 – Source : Wikipedia

- Le **stockage sur semi-conducteur à l'état solide**, aussi appelé mémoire Flash. Elle est constituée de transistors à effet de champ à grille métal-oxyde ou MOS (*Metal Oxide Semiconductor Field Effect Transistor*). L'information y est stockée grâce au piégeage d'électrons dans une grille flottante au sein de la cellule constituant le transistor.

  D'abord utilisée en tant que mémoire de microcontrôleur[5], puis pour le stockage amovible USB, elle est apparue comme une alternative aux disques durs traditionnels sous forme de "disques" SSD (*Solid State Drive*) qui réunissent une grande quantité de transistors MOS (il n'y a concrètement aucun plateau). Leurs meilleures performances en termes de résistance aux chocs[6], débit, latence et consommation électrique, leur font prendre une part de plus en plus importante du stockage de données dans les ordinateurs comme dans les datacenters, même si le rapport capacité/coût d'achat reste encore à l'avantage des disques durs.

Disque SSD, avec ses cellules de mémoire flash – Source : tomshardware.com

[5] Un microcontrôleur est un circuit intégré qui rassemble les éléments essentiels d'un ordinateur : processeur, mémoires, unités périphériques et interfaces d'entrées-sorties.

[6] Contrairement aux disques durs, les disques SSD sont dépourvus d'éléments mobiles

- Le **stockage optique** : principalement utilisé pour les supports amovibles, le stockage optique correspond aux disques compacts (CD), DVD et aujourd'hui le Blu-ray. Ce stockage disparaît peu à peu au profit d'autres formes de stockage amovible ou d'autres formes de transmission des données, directement par les réseaux.

  L'avenir du stockage de masse doit donc d'abord passer par des innovations sur les technologies actuelles de stockage. On peut notamment citer :

  - Les disques durs à hélium : L'hélium étant un gaz 7 fois moins dense que l'air, il a été proposé de créer d'utiliser ce gaz au sein de disques durs traditionnels. Les plateaux au sein de tels disques font face à moins de résistance et ne rencontrent presque aucune turbulence, permettant d'augmenter le nombre de plateaux, en sus d'augmenter leur densité. Les premiers disques à hélium sont apparus sur le marché en 2013, mais ils n'ont pas remplacé les risques à air : ils restent limités aux disques à haute capacité, en raison de leur coût.
  - La mémoire NAND verticale ou 3D : elle consiste en une superposition verticale de cellules, à l'opposé de l'approche traditionnelle visant la miniaturisation et le regroupement du plus grand nombre de transistors sur un même plan (qui se heurte aux interférences que provoquent les cellules entre elles).

  À côté de ces innovations sur les technologies actuelles, l'émergence et le développement de technologies de rupture reste indispensable pour permettre aux capacités de stockage de suivre, tant que possible, le rythme de l'évolution du volume des données.

2. Technologies de rupture

Trois principales technologies de rupture se profilent actuellement : le stockage ADN, le stockage optique dit "5D" et le stockage sur aimants mono-moléculaires.

Le stockage ADN propose un changement d'approche particulièrement radicale au stockage de données : utiliser le vivant comme médium. Il s'agirait ainsi d'encoder l'information sur les paires de bases nucléiques (A-T-C-G). La molécule d'ADN constituée serait stockée dans une capsule en verre, elle-même protégée dans une capsule en acier.

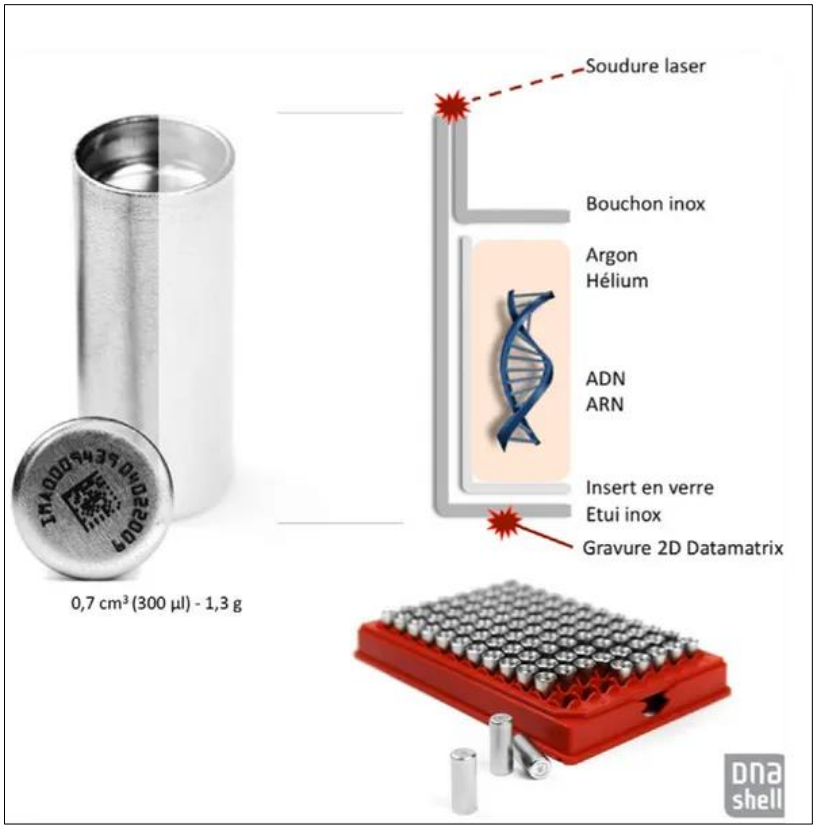
- Avantages : Ce stockage permettrait un stockage extrêmement stable sur des décennies à température ambiantes - et potentiellement des milliers d'années à plus basse température[7] - tout en permettant une capacité de stockage absolument gigantesque : sous forme ADN, l'ensemble des données de l'humanité tiendrait dans le coffre arrière d'une fourgonnette.
- Inconvénients : le coût et la lenteur des procédés de lecture (séquençage) et d'écriture (synthèse) sur les bases nucléïques.

Le premier encodage ADN réussi date de 2012. D'après François Képès, chercheur biologiste et membre de l'Académie des technologies, il faudra attendre au moins 5 ans pour que les coûts et la vitesse deviennent acceptables pour la lecture ADN (séquençage), mais il faudra en revanche plutôt une quinzaine d'années du côté de l'écriture (synthèse)[8]. Dans cette attente, 15 entreprises dont Microsoft, Illumina, Twist Bioscience et Western Digital se sont rejointes en 2020 dans le cadre d'une initiative visant à développer les standards de cette technologie.

[7] https://www.sciencemag.org/news/2017/03/dna-could-store-all-worlds-data-one-room

[8] https://www.science-et-vie.com/technos-et-futur/vos-photos-et-videos-peuvent-etre-conservees-sur-de-l-adn-60431

À court et moyen terme, l'ADN est une solution de stockage pour les données auxquelles on n'a pas besoin d'accéder régulièrement, et concerne donc davantage les besoins d'archives et de sauvegarde. On envisage cependant également de réaliser des traitements sur les données directement sous forme ADN.



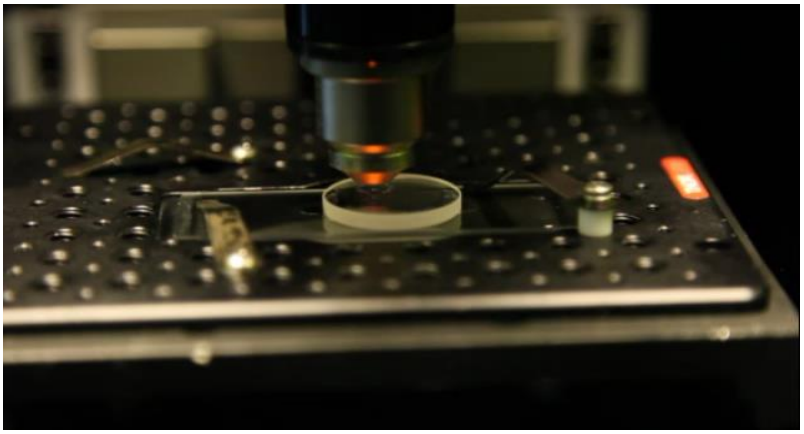
Capsule de stockage ADN de données – Source : Science & Vie

Le stockage optique 5D sur quartz vise à coder l'information au sein de quartz. L'écriture est réalisée par des laser femtoseconde[9] et repose sur la forme des nanostructures gravées, leur taille et leur orientation.

- Avantages : Une capacité de stockage extrême. Une durée de vie théorique de 14 milliards d'années, et une résistance aux radiations cosmiques et aux hautes températures (jusqu'à 1000°c).
- Inconvénients : l'approche WORM (*Write-Once, Read Many*) qu'impose cette technologie, qui ne permet pas la réécriture de données.

Cette technologie est d'ores et déjà utilisée par la Arch Mission Foundation, qui vise à créer des archives de l'ensemble du savoir humain et à en envoyer le plus grand nombre en divers lieux du système solaire. Github, filiale de Microsoft, prévoit en outre d'utiliser cette technologie pour archiver l'ensemble de ses dépôts (*repositories*) de données. De façon générale, l'approche WORM en fait un candidat idéal pour le stockage de données avec un besoin d'intégrité maximale, puisqu'il ne permet par définition par la réécriture : un adversaire ne pourrait pas modifier ou détruire les données de sauvegarde, quant bien même celles-ci lui seraient accessibles.

[9] Un laser femtoseconde produit des impulsions ultra courtes, de l'ordre de quelques femtosecondes (10^{-15} s).



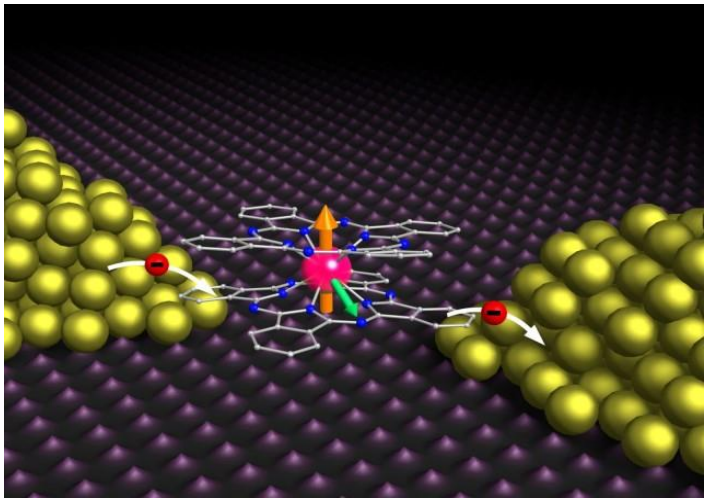
Inscription de données sur un disque de quartz au centre de recherche optoélectronique de l'Université de Southampton

Source : Extreme Tech

Le stockage à froid SMM (*Single Molecule Magnets*) est une méthode de stockage de données à l'échelle nanométrique, sur des aimants mono-moléculaires comme son nom l'indique[10].

- Avantages : Une très haute densité de stockage, pour des vitesses de lecture et d'écriture que l'on peut supposer similaires aux technologies traditionnelles de stockage : on imagine notamment utiliser des couches de SMM sur les plateaux de disques durs.
- Inconvénients : la barrière de la température (-269°c par exemple dans le cadre du projet PhotoSMM, conçu par des chercheurs de l'Institut des sciences chimiques de Rennes en collaboration avec une équipe de l'Université Berkley).

Le domaine est encore trop expérimental pour déterminer de cas d'usages préférentiels. Au-delà du stockage d'information au format classique, les aimants mono-moléculaires sont un candidat privilégié au stockage d'information dans le domaine de l'informatique quantique.



Un atome de terbium (en rose) entre deux molécules organiques (en gris et bleu), formant un aimant mono-moléculaire.

Source : Institut technologique de Karlsruhe

[10] https://cordis.europa.eu/article/id/123263-scientists-introduce-the-data-storage-of-the-future/fr

D’autres pistes technologiques devraient également trouver des applications dans le stockage de données, comme par exemple le remplacement du silicon par du graphène comme matériau de base des circuits électroniques. Découvert en 2004, ce matériau constitué d’une unique couche d’atome de carbone possède un fort potentiel : 200 fois plus solide que l’acier et 250 fois plus conducteur d’électricité que le silicon[11], il permettrait donc de réduire la consommation électrique. Malheureusement, cette perspective reste encore très éloignée. S’il s’agit bien d’une piste majeure - l’Union Européenne a ainsi démarré le Graphene Project en 2013 avec un milliard d’euros d’investissement sur 10 ans, il faut savoir qu’il faut compter en règle générale entre 30 à 40 ans pour qu’un nouveau matériau intègre les produits finaux.

Conclusion

Il est évidemment très difficile de préjuger de la maturité potentielle de technologies de rupture à horizon 20 ans, mais il est clair qu’elles sont très attendues pour faire face à la problématique de plafond de capacités de stockage.

Du côté du stockage à froid de données statiques, les avancées des technologies de stockage ADN et optiques sur quartz sont très encourageantes et rassurent sur les capacités à stocker des données de façon sensiblement illimitée.

En revanche, le stockage de données dynamiques, réelles sources de consommation énergétique, se profile comme une problématique majeure. Les aimants mono-moléculaires semblent être un excellent candidat, mais leur usage hors laboratoire est particulièrement lointain, ne serait-ce que du fait des exigences extrêmes de température. Pour de nombreuses années, il faudra se contenter d’innovations incrémentales sur les méthodes de stockage actuelles, qui ne fourniront pas une capacité répondant à la croissance exponentielle de la demande. Ce faisant, l’industrie cherche à réaliser des optimisations sur d’autres tableaux. Sur le plan énergétique, cela passe par exemple par des choix de localisation de datacenters dans les climats les plus froids possibles ou par le stockage en mer[12].

A terme cependant, ces technologies de rupture ont vocation à devenir incontournables. Elles pourraient constituer une opportunité pour l’Europe de construire sa propre industrie “silicone” et de sortir de sa dépendance aux producteurs américains et asiatiques.

[11] https://futurism.com/graphene-computers-work-1000-times-faster-use-far-less-power
[12] https://news.microsoft.com/innovation-stories/project-natick-underwater-datacenter/

ANALYSES (2/2)

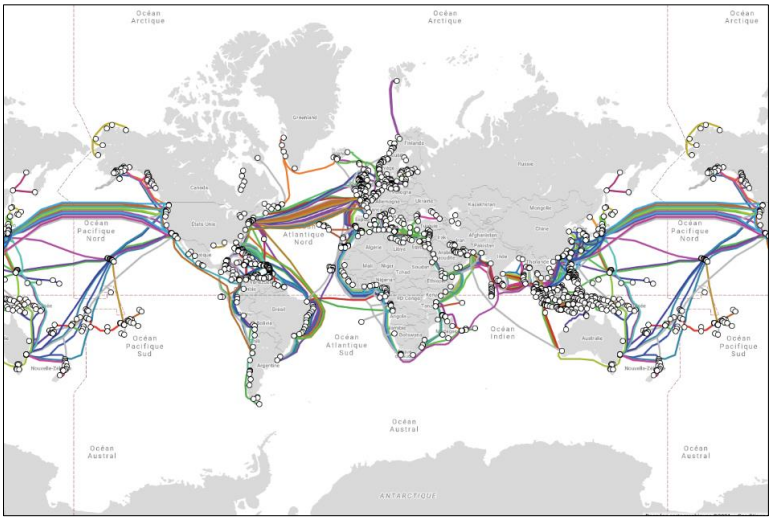
LES CABLES SOUS-MARINS : UNE INFRASTRUCTURE MÉCONNUE MAIS STRATÉGIQUE

Les câbles sous-marins sont aujourd'hui des infrastructures vitales et hautement stratégiques à l'échelle mondiale. L'accélération de la transformation numérique des organisations, l'augmentation continue du nombre d'internautes, ainsi que l'essor des objets connectés et de l'industrie 4.0, constituent autant de développements rendus possibles par ces câbles.

Chaque évolution technologique en matière de communication a vu l'apparition de nouveaux types de câbles sous-marins. Le premier câble sous-marin télégraphique transatlantique a été posé en 1858. Il faudra ensuite attendre 1956 pour que le câble téléphonique voie le jour. Enfin, les premiers câbles à fibre optique ont été déployés à partir de 1988. Ces câbles, qui ont rapidement acquis une place centrale dans le développement de moyens et de canaux de communication à l'échelle mondiale, assurent aujourd'hui le passage de tous types de signaux, du téléphonique au fax en passant par Internet (y compris haut débit), la photo, la vidéo et la télévision numérique haute définition. En 2021, environ 426 câbles étaient en service dans le monde pour un total de plus de 1,3 million de kilomètres[13].

Une partie du fonctionnement des États et de leurs économies repose aujourd'hui sur ces routes d'échanges numériques, aujourd'hui essentiellement maritimes puisque moins de 1% des communications téléphoniques transitent par la voie satellite.

Historiquement, les câbles sous-marins étaient la propriété des entreprises - privées ou publiques - de télécommunication. Depuis 2016, les géants du numérique, les fameux GAFAM (Google, Apple, Facebook, Amazon, Microsoft) possèdent ou louent plus de la moitié de la capacité de ces câbles. Ces nouveaux acteurs, en arrivant progressivement sur le marché des câbles sous-marins, se dotent ainsi de leviers d'influence grandissante sur les États et les autres entreprises du secteur des télécommunications.



Source : Submarine Cable Map

[13] « Submarine Cable 101 », Telegeography [En ligne]

Les câbles sous-marins, enjeux économiques et politiques

Bien que le secteur du câble sous-marin soit essentiel à l'activité et à l'économie mondiale, son chiffre d'affaires global est en réalité peu élevé. Celui-ci avoisine les 3 milliards de dollars, un montant relativement faible compte-tenu du caractère stratégique et incontournable de ces câbles. Environ 100 fois plus économique que le satellite, la majorité du coût d'un câble réside dans sa fabrication et sa pose.

Les câbles sous-marins, un enjeu stratégique pour les États

Si les câbles sous-marins représentent un investissement considérable, ils sont aussi la promesse de retombées économiques, industrielles et commerciales significatives aux États qui en autorisent le passage ou l'atterrissage sur leur territoire. Il existe par conséquent une réelle compétition entre les États pour convaincre à leur profit les entreprises chargées de leur déploiement. Du côté de ces opérateurs justement, le choix du point d'atterrissage prend un compte un certain nombre de critères dont l'environnement économique ce territoire, la présence d'infrastructures permettant de router le câble vers les *data centers,* la régulation nationale en vigueur, ou encore la volonté politique du gouvernement concerné.

Pour l'État ou le territoire sélectionné, l'atterrissage d'un câble sous-marin permet d'abord la consolidation ou le développement d'un écosystème industriel lié aux échanges numériques (stockage, transmission, acheminement, échange…). C'est le cas en France de Marseille, 9ème hub Internet mondial selon Telegeography, qui fait figure de « porte d'accès numérique »14 entre l'Europe, l'Afrique, le Moyen-Orient et l'Asie. Point d'atterrissage de 14 câbles sous-marins, 6 points d'échanges internet (IXP), la ville héberge aussi 14 plates-formes et réseaux de distribution de contenu et 160 opérateurs de télécommunications internationaux et nationaux. Une véritable communauté industrielle s'est ainsi structurée autour de ce point d'atterrissage, pour le relier et l'interconnecter à divers *data centers* de la région.

Mais le simple passage, ou la simple pose, d'un câble sur le sol des fonds marins des États qui l'autorisent est déjà un atout financier et une source de revenus non négligeables, puisque les États en question reçoivent en contrepartie des redevances conséquentes. À titre d'exemple, l'Égypte perçoit des redevances pour les droits aussi bien de transit des câbles sous-marins dans le canal de Suez, que d'atterrissage[15] à Alexandrie.

Pour un État comme pour une entreprise, contrôler un câble sous-marin permet aussi de contrôler les flux de données qui y transitent. Un atout politique de poids, car il permet par la même d'affecter la maîtrise de l'information par les utilisateurs de ces câbles. Sur le plan militaire, les câbles sous-marins peuvent donc même devenir un enjeu de supériorité opérationnelle. Les premiers exemples remontent à la Première Guerre mondiale : le Royaume-Uni disposait d'un réseau très développé qui lui a permis de maintenir ses communications tout en interrompant régulièrement celles de l'Allemagne. Sur le plan politique, les câbles sont, comme de manière plus larges les infrastructures numériques, un enjeu de souveraineté et d'indépendance qu'il est indispensable de protéger de ses concurrents ou adversaires[16].

Preuve de l'enjeu que les câbles sous-marins représentent, les principaux acteurs étatiques se sont positionnés sur le secteur. La France, via Orange Marine et Alcatel Submarine Network notamment, et les États-Unis via TE SubCom, représentent aujourd'hui à eux seuls 30% de parts de marché respectivement en matière de fabrication et de pose des câbles. De son côté, la Chine, qui s'était jusqu'à présent concentrée sur les câbles militaires équipés d'hydrophones pour enregistrer la signature des navires et des sous-marins,

---

14 https://www.nouvellespublications.com/marseille-la-future-autoroute-numerique-chinoise-arrivera-au-prado-en-2021-2702.html

15 Lieu d'arrivée et de raccordement du câble sur le rivage.

16 « Le devoir de souveraineté numérique », Gérard Longuet, rapport n°7, Sénat [En ligne], 1er octobre 2019

commence progressivement à pénétrer le marché. L'entreprise Huawei Marine a lancé plus d'une centaine de projets de construction ou de modernisation de câbles à fibre optique, avant de faire l'objet d'un embargo américain, freinant ainsi les ambitions chinoises. Pour autant, la cession en juin 2020 de 51% des parts de l'entreprise à Hengtong Optic-Electric (Chine) a permis à Pékin de contourner les sanctions et de poursuivre ses projets.

À ces acteurs historiques viennent aujourd'hui s'ajouter de nouveaux entrants, notamment les « GAFAM », qui disposent des capacités financières suffisantes pour se lancer de manière autonome dans la pose et l'exploitation de câbles sous-marins à fibre optique.

Les nouveaux entrants, un défi à la souveraineté des États ?

L'écosystème des câbles sous-marins comprend deux catégories d'acteurs :

- Les constructeurs : il s'agit de sociétés qui maîtrisent la technologie des câbles sous-marins et qui sont capables de les construire ainsi que l'ensemble des équipements électroniques leur permettant de fonctionner. Il existe quatre acteurs majeurs dans ce domaine : SubCom (États-Unis), Alcatel Submarine Network (France), NEC (Japon), Huawei Marine (Chine) ;
- Les bailleurs : il s'agit des gouvernements, des opérateurs, des acteurs privés individuels qui réalisent des opérations financières et plus récemment des GAFAM qui sont principalement présents sur deux grands terrains de bataille : la route transatlantique et transpacifique.

Depuis 2016, les géants du numérique ont investi de lourdes sommes et sont aujourd'hui propriétaires ou locataires de plus de la moitié de la capacité des câbles sous-marins, concurrençant directement les États sur un secteur dont ils avaient l'apanage.

En effet, les GAFAM réalisent environ 50% des investissements dans le secteur des câbles sous-marins. Google en est le principal contributeur, avec le financement de 14 câbles dans le monde, dont 2 câbles financés seul. En 2019, l'entreprise américaine a d'ailleurs annoncé la construction d'un troisième câble sous-marin sur financement privé, Equiano[17], qui reliera le Portugal et l'Afrique du Sud en longeant la côte ouest du continent africain. Selon Google, Equiano devrait offrir 20 fois plus de capacité réseau que le dernier câble construit, WACS, pour desservir la région. La construction d'un câble sur financement privé représente l'avantage pour la société concernée, de ne pas avoir à négocier le point d'atterrissage avec d'autres co-financeurs et de gagner en efficacité, par exemple en connectant plus directement ses propres *data centers*. Google est suivi de près par Facebook (détenteur de 10 câbles), puis par Microsoft (4 câbles) et Amazon (3 câbles).

Si les GAFAM souhaitent disposer de leurs propres câbles sous-marins, c'est que leurs activités requièrent un débit Internet considérable que les câbles existants ne peuvent plus offrir pour des raisons de capacités[18]. Alors que les acteurs traditionnels du secteur, tels qu'Orange, privilégient la constitution de larges consortiums pour la construction de câbles, et ce afin de partager l'investissement financier associé, les GAFAM semblent quant à eux opter pour les regroupements réduits, ou bien développent seuls ces câbles afin de conserver le monopole décisionnel sur le processus de construction et déploiement. Par exemple, le projet Africa Coast to Europe (ACE) appartient à un consortium de 19 entreprises des télécommunications, tandis que le câble

[17] « Introducing Equiano, a subsea cable from Portugal to South Africa", Google [En ligne], 28 juin 2019
[18] « Google and Facebook are gobbling up the internet's subsea cables", Wired [En ligne], 18 novembre 2018

MAREA, qui relie les États-Unis à l'Espagne, est uniquement géré par Facebook, Microsoft et Telxius[19]. À noter que la capacité de bande passante déployée par les câbles détenus par Google, Facebook, Microsoft et Amazon (en propre ou en consortiums) a été multipliée par 10 entre 2013 et 2017. MAREA disposait notamment d'une capacité initiale de 160 térabits par seconde (Tb/s), aujourd'hui elle dépasserait les 200 Tb/s. En comparaison, ACE présente une capacité de 5 Tb/s.

L'arrivée de ces géants du numérique pose cependant la question de la dépendance des États, et plus largement de leurs sociétés, à ces entreprises privées dont on peut craindre à terme qu'elles soient en position de monopole tant leurs services et produits sont utilisés dans le monde. Cette situation donne aux GAFAM une marge de manœuvre non négligeable pour agir et décider de l'emploi des câbles. Ils disposent par ailleurs, contrairement à d'autres acteurs privés comme publics, de leviers financiers pour le développement de nouveaux projets de câbles. À titre d'exemple, Facebook devrait consacrer 5 milliards de dollars pour le déploiement de câbles entre 2018 et 2023. De plus, d'ici quelques mois, environ 95% de la capacité totale de télécommunications transitant sous l'Atlantique devrait être contrôlée par les GAFAM[20], annonçant peut-être une forme de privatisation progressive d'une partie d'Internet au profit de quelques acteurs privés.

Des infrastructures aussi indispensables que vulnérables

Les convoitises dont les câbles font l'objet sont autant de fragilités, et ce d'autant que la cartographie des câbles a toujours été connue de manière précise, au « mètre près », en dehors bien sûr des câbles à usage purement militaire. Mais les câbles sous-marins sont également particulièrement vulnérables face aux menaces naturelles.

La menace naturelle et accidentelle

La première fragilité d'un câble sous-marin réside dans sa nature même. Puisqu'il repose sur les fonds marins et n'est enfoui que lorsque cela est nécessaire, comme par exemple en eau peu profonde, il est particulièrement exposé aux catastrophes naturelles. Par exemple, le tsunami qui a touché le Japon en 2011 a gravement endommagé le réseau des câbles de la région et a contraint Tokyo à réorganiser le trafic entre différents points du pays. Pour mieux protéger ces câbles, certains pays ont mis en place des zones de protection dans lesquelles le trafic maritime est strictement encadré afin d'éviter toute dégradation fortuite. Par exemple, la France surveille les câbliers qui travaillent dans ses espaces maritimes. Pour autant, des entreprises telles qu'Orange Marine et Alcatel Submarine Network assurent elles-mêmes le contrôles de leurs propres câbles afin de déceler et de localiser des coupures ou des dégradations.

Les câbles sous-marins restent également vulnérables aux activités de pêche, les ancres et les filets des navires étant régulièrement à l'origine d'incidents involontaires. Ainsi en décembre 2008, trois câbles sous-marins situés à une profondeur de 200 à 400 mètres ont été rompus au niveau de la Tunisie sur des segments reliant la Sicile et l'Égypte. France Télécom avait alors à l'époque évoqué l'hypothèse d'une ancre de bateau.

Le sabotage à motivation financière

En raison de leur localisation précise et publique, et de leur insuffisante protection, les câbles sous-marins restent des cibles relativement aisées pour des acteurs mal intentionnés et disposant des moyens de les

[19] « Câbles sous-marins : Les nouveaux pouvoirs des géants du numérique », Institut Rousseau [En ligne], 26 août 2020
[20] « Connectivité Internationale : la guerre des câbles sous-marins », PDJ – Observatoire du FIC [Replay], 27 janvier 2021

endommager volontairement. En Afrique, une pratique courante est le sabotage pour la revente de câbles. C'est ainsi qu'en 2007 des pêcheurs vietnamiens ont coupé plus de 500 kilomètres de câbles pour récupérer les matériaux composites et les revendre. En conséquence, le Vietnam a perdu plus de 80% de sa connectivité.

Conscient de cette menace, l'OTAN a même intégré un cas de sabotage de câbles au large des côtes françaises et britanniques à son exercice de cyberdéfense. Le scénario était basé sur un sabotage commandité par un pays ennemi et réalisé par un bateau de pêche laissant volontairement traîner son ancre, dans le but de provoquer une coupure majeure d'Internet en France et en Europe.

L'espionnage

L'une des vulnérabilités régulièrement relevées aujourd'hui concerne les activités d'espionnage. L'accès au flux de données transitant dans les câbles constitue en effet, depuis l'ère du télégraphe électrique, un véritable enjeu pour les agences de renseignement. Ces dernières bénéficient *a priori* toutes d'un cadre juridique leur permettant de collecter les données de tout câble traversant leur territoire national.

Si la première mise sur écoute connue d'un câble sous-marin par la NSA américaine (National Security Agency) date de l'opération Ivy Bell en 1971, la mise en lumière de la possibilité d'accès aux câble sous-marins à des fins de renseignement a eu lieu en 2013. L'affaire Snowden a en effet montré l'ampleur avec laquelle le Government Communications Headquarters (GCHQ) britannique et la NSA pratiquaient cette méthode de collecte de données avec le programme "Upstream"[21]. D'autant que la configuration du réseau international de câbles fait du Royaume-Uni une plaque tournante des télécommunications mondiales.

La cyberattaque à finalité politique

Comme tout système connecté à Internet, les câbles sous-marins sont sensibles aux cyberattaques. Les technologies de gestion à distance permettent aux opérateurs de câbles d'interconnecter les câbles sous-marins, les points d'accès et les différents composants intervenant dans l'architecture du système. Ces systèmes de gestion de réseau sont généralement fournis par les sociétés chargées de poser les câbles. Des cyberattaques contre les systèmes de gestion de réseaux et les Internet Exchange Points (IXP)[22] peuvent perturber les échanges voire la connectivité de régions entières.

Les câbles sous-marins jouent aujourd'hui un rôle essentiel dans les communications, en particulier dans les accès à Internet. Ils constituent, plus largement, des enjeux économiques et politiques majeurs pour les États les déployant ou accueillant leurs « points d'atterrissages ». L'essor du numérique et son développement croissant ne font qu'accroitre la dépendance des États, des organisations et plus largement des sociétés à ces câbles. Leurs dégradations volontaires ou involontaires, la saturation des réseaux, les coupures étatiques, les phénomènes climatiques, les utilisations frauduleuses de données personnelles, la surveillance des populations etc. peuvent être à l'origine de failles de sécurité fortement préjudiciables pour les États.

[21] « Un océan de câbles : Menaces sous les mers, panique dans le cyberespace », RFI [En ligne], mars 2019

[22] Infrastructure physique permettant aux fournisseurs d'accès d'échanger du trafic Internet entre leurs réseaux de systèmes autonomes grâce à des accords de « peering ».

FOCUS INNOVATION

GitGuardian : une nouvelle réponse aux enjeux de la sécurité applicative

Entretien avec Carole Winqwist, Chief Marketing Officer de GitGuardian.

Présentation

GitGuardian est une jeune pousse française créée en 2017 par deux co-fondateurs issus de l'École centrale Paris, Jérémy Thomas (CEO) et Éric Fourrier (CTO).

Passionnés de développement logiciel, ils se sont d'abord lancés dans la détection de « secrets » (informations d'authentification utilisées de façon programmatique dans un logiciel ou une application, par exemple pour permettre l'accès à un système de paiement) dans le code source sur GitHub, plateforme de partage de code utilisée par +50 millions de développeurs. Témoins du nombre significatif de « secrets » publiquement accessibles et pouvant être détournés à des fins malveillantes par des pirates, et conscients du changement radical de la façon dont les sociétés développent un logiciel, leur expérience sur GitHub s'est transformée en un véritable projet d'entreprise.

Leur petite structure a rapidement pu compter sur l'appui de business angels tels que Scott Chacon (GitHub) et Solomon Hykes (Docker), leur permettant de mettre en place un premier produit, GitGuardian Public Monitoring, capable de détecter les « secrets » ayant fuité sur le GitHub public, puis un second produit, GitGuardian Internal Monitoring permettant de scanner les dépôts de code internes des entreprises.

Avec une levée de fonds de 12M$ fin 2019 (série A), menée par Balderton Capital avec la participation des business angels historiques et de BPI France, la société compte aujourd'hui 35 salariés et se donne pour ambition de répondre aux enjeux de la sécurité applicative via la détection de secrets[23], avec l'objectif final de sécuriser le code source des entreprises tout en soutenant et en éduquant les développeurs.

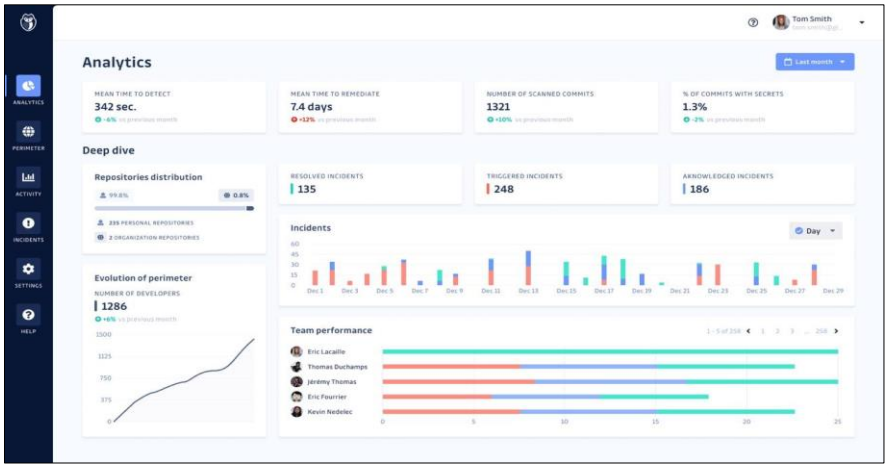
Solution

En utilisant un moteur de détection unique embarquant de l'Intelligence artificielle (IA), GitGuardian surveille les dépôts de code, c'est-à-dire le code déposé sur un VCS (Version Control System) comme GitHub, GitLab ou Bitbucket, par les développeurs.

[23] « State of Secret Sprawl on GitHub », rapport 2021, GitGuardian. Types de secrets trouvés en 2020 : 27,6% clés Google / 15,9% outils de développement (Django, RapidAPI, Okta) / 15,4% stockage de données (MySQL, Mongo, Postgres…) / 12% autres (y compris CRM, Cryptos, fournisseurs d'identité, systèmes de paiement, surveillance) / 11,1% systèmes de messagerie (Discord, Sendgrid, Mailgun, Slack, Telegram, Twilio…) / 8,4% fournisseurs de services dans le cloud (AWS, Azure, Google, Tencent, Alibaba…) / 6,7% clés privées / 1,9% réseaux sociaux / 0,8% plate-forme de contrôle de version (GitHub, GitLab) / 0,4% outils de collaboration (Asana, Atlassian, Jira, Trello, Zendesk…)

D'une part, GitGuardian Public Monitoring (offre SaaS) scanne, via un algorithme, les dépôts de code accessibles publiquement sur GitHub[24]. Les entreprises peuvent ainsi surveiller leurs dépôts de code mais aussi les dépôts de code publics de leurs développeurs. Lorsqu'un secret est détecté, GitGuardian alerte le développeur à l'origine du dépôt de code suspect ainsi que l'équipe de sécurité (pour les clients Entreprise). La remédiation peut ainsi commencer rapidement s'il s'agit en effet d'un « secret » publié par erreur. Grâce au *machine learning,* l'algorithme de GitGuardian devient plus précis en apprenant des suites données à ses alertes (classement déclaratif en vrai positif ou faux positif, ou classement par analyse du comportement du développeur : effacement ou passage en privé du code). Le moteur de détection de GitGuardian est composé aujourd'hui de plus de 250 « détecteurs ».

Dans son produit destiné à la surveillance des dépôts de code internes d'une entreprise, GitGuardian intervient sur le périmètre de l'organisation : SI, applications, logiciels… Il s'agit alors d'une offre SaaS ou *on-premise*. L'objectif est d'abord d'éviter l'exposition de secrets, notamment lors des développements logiciels et applicatifs de l'entreprise. La plupart des organisations estiment qu'elles sont protégées dès lors qu'elles opèrent dans leurs dépôts internes. Elles ne prennent pas en compte le fait qu'un code et les secrets qu'il peut contenir peuvent se retrouver très rapidement dans plein d'endroits par le biais de copier/coller et de réutilisation. À cela s'ajoute l'utilisation croissante de messageries type Slack, sur lesquelles les collaborateurs échangent régulièrement des clés sans penser qu'elles peuvent être exposées. L'exposition des secrets en clair augmente la surface d'attaque des entreprises en permettant à des acteurs malveillants de se déplacer latéralement dans les systèmes et intensifie donc nettement les risques. L'entreprise choisit, dans GitGuardian Internal Monitoring, le périmètre de surveillance et dispose d'un Dashboard qui permet une collaboration entre les équipes de sécurité et les développeurs (voir ci-dessous).



Dashboard GitGuardian

La solution est enfin conçue comme un outil éducatif, car elle met le développeur dans la boucle de remédiation. L'objectif n'est pas en effet de stigmatiser ou sanctionner les développeurs à l'origine d'un dépôt de code malencontreux, mais de les sensibiliser aux risques, et de les aider, le cas échéant, à détecter un

[24] « State of Secret Sprawl on GitHub », rapport 2021, GitGuardian : 15% des fuites sur GitHub se produisent dans des dépôts publics appartenant à des organisations et 85% des fuites se produisent dans des dépôts personnels des développeurs.

secret publié par erreur, le supprimer, en nettoyer l'historique, et ainsi éviter une remédiation longue et coûteuse pour l'entreprise.

Perspectives

Si leur solution est aujourd'hui utilisée à 90% par le marché américain, GitGuardian entend également s'adresser aux marchés français et européen. La société considère en effet que le manque de maturité de ces deux marchés, initialement en retard sur leur voisin outre-Atlantique sur les problématiques DevOps (système de production de code itératif et rapide) d'une part et architectures distribuées (services répartis / composants isolés) d'autre part, est désormais en train de se résorber.

Avec la généralisation des solutions Cloud, les architectures distribuées sont d'ailleurs de plus en plus présentes dans les institutions publiques, dont le ministère des Armées en France, qui font donc appel à de nombreux prestataires externes et s'exposent *de facto* aux mêmes risques que les entreprises.

GitGuardian travaille actuellement sur deux développements : l'extension du périmètre de détection (données personnelles, de santé et propriété intellectuelle), et l'extension des outils et services utilisés par l'entreprise (logiciels, applications…) disponibles sur le Dashboard (analyse des messageries internes par exemple).

CALENDRIER

21/04/2021 – PFUE : QUEL RÔLE POUR LA CYBERDÉFENSE MILITAIRE EN EUROPE ? (VISIOCONFÉRENCE)

Organisé par **CEIS (Avisa Partners)** au profit du **Commandement de la cyberdéfense**, un petit-déjeuner-débat en visioconférence sur le sujet « **PFUE : quel rôle pour la cyberdéfense militaire en Europe ?** » aura lieu le **mercredi 21 avril de 8h30 à 10h00**.

Le cyberespace est le théâtre d'une conflictualité débridée et assumée où s'affrontent des acteurs privés comme publics. L'Union européenne, dont les progrès de ces dernières années en matière de cybersécurité (directive NIS, boîte à outils cyber-diplomatiques, réseaux de coopération entre États membres…) la propulsent comme un acteur majeur, ambitionne également de s'imposer en acteur incontournable de la cyberdéfense. Les enjeux sont nombreux : il s'agit à la fois d'assurer sa propre sécurité, ainsi que sa résilience et celle des États membres, et de développer une souveraineté numérique.

Si le domaine civil semble habité d'une dynamique importante, qu'en est-il de la dimension défense, développée au travers de la Politique de sécurité et de défense commune (PSDC) ?

Alors que la France s'apprête à prendre la présidence du Conseil de l'Union européenne en janvier 2022, quel rôle peut-elle jouer pour accompagner et accélérer la montée en puissance de la cyberdéfense militaire en Europe ? Comment peut-elle contribuer à l'affirmation d'une Europe souveraine et indépendante en matière de cyberdéfense et plus largement de numérique ?

Nous accueillerons notamment pour en discuter le **colonel Philippe Pacom**, expert national C4ISR & Cyber à la Délégation militaire française à l'Union européenne, et le **commandant Nicolas Chevrier**, en charge de la coopération internationale au Commandement de la cyberdéfense.

Inscrivez-vous directement sur la page Livestorm de l'événement (nombre de places limité).

ACTUALITÉ

L'ADMINISTRATION BIDEN PUBLIE LA FEUILLE DE ROUTE DE SA STRATEGIE DE SECURITE NATIONALE

La Maison Blanche a publié le 3 mars 2021 son *Interim National Security Strategic Guidance*. Ces directives provisoires visent à exposer la vision du Président Joe Biden sur la place des États-Unis dans le monde, ainsi qu'à encadrer d'ores et déjà l'action du gouvernement américain, en attendant la publication de la stratégie de sécurité nationale *a priori* en juin prochain.

Cette feuille de route dresse un état des lieux des principales menaces dans le monde, qui ont la particularité de ne respecter « ni frontières, ni murs », à commencer par les pandémies et les autres risques biologiques. Le document identifie également la crise climatique, les menaces cyber et numériques, les perturbations économiques, les crises humanitaires, l'extrémisme violent et le terrorisme, ainsi que la prolifération des armes nucléaires et de destruction massive.

L'administration Biden souhaite faire de la cybersécurité l'une de ses priorités. Son objectif est avant tout la construction d'un environnement en ligne sûr et sécurisé pour tous les Américains. Dans ce cadre, elle souhaite, outre renforcer les synergies entre les secteurs public et privé, augmenter les investissements dédiés à la filière, aussi bien en termes d'infrastructures que de métiers.

Sur le plan international, les États-Unis affirment avec ce document leur intention de préserver les démocraties des cyberattaques, de la désinformation et de « l'autoritarisme numérique ». Ils soulignent à cet égard leur volonté de travailler aux côtés des alliés et des partenaires pour faire respecter les normes existantes dans le cyberespace, en plus d'en élaborer de nouvelles. Dans le domaine opérationnel, l'administration Biden affiche sa prédisposition à répondre de manière « rapide et proportionnelle » aux cyberattaques adverses, par le recours à des moyens de cyberdéfense ou non.

Pour accéder au document *Interim National Security Strategic Guidance*, cliquez ici.

La **Direction générale des relations internationales et de la stratégie (DGRIS)** propose des 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 les organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

À ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique (OMC)**, qui s'inscrit dans le contrat-cadre n°2018-02. 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 | 75015 Paris

CEIS
Tour Montparnasse | 33 avenue du Maine | 75015 Paris
E-mail : omc@ceis.eu