Lettre mensuelle – Avril 2020 – Disponible sur omc.ceis.eu

Table des matières

ANALYSES (1/2)

ANALYSE COMPORTEMENTALE : DÉTECTER LES INCIDENTS GRÂCE AU MACHINE LEARNING

En octobre 2019, Guillaume Poupard, le directeur général de l'Agence nationale pour la sécurité des systèmes d'information (ANSSI), identifiait un point faible dans la protection des systèmes de sécurité : la détection des intrusions, qui, dans 35 % des cas, survient entre six et neuf mois seulement après l'intrusion[1].

Historiquement, la détection des intrusions repose sur des signatures statiques, qui décrivent les signes de la présence d'une activité malveillante dans un système. Plus précisément elle permet de reconnaître, dans le fonctionnement et les activités d'un système, des comportements malveillants ou des empreintes (hashes, adresses IP…) déjà associés à des actes malveillants. Cette méthode permet ainsi de faire remonter des alertes dites « explicites », ou qualifiées, c'est-à-dire qui identifient précisément l'acte malveillant, mais se limite en revanche aux modes opératoires déjà identifié précédemment comme malveillants.

Or les empreintes et indicateurs sur lesquels repose cette méthode évoluent extrêmement rapidement : les hashes, par exemple, peuvent être modifiés à chaque compilation du code. D'autre part, les attaques sont de plus en plus nombreuses et sophistiquées, ce qui rend les signatures rapidement obsolètes et explique en partie le faible taux de détection des intrusions. Les Security Operations Center (SOC) sont donc forcés de reconsidérer leur approche.

Un changement d'approche dans la détection des intrusions

La détection des intrusions peut être envisagée sous un autre angle : celui de l'analyse comportementale. Contrairement aux signatures statiques, les algorithmes d'analyse comportementale ne permettent pas de qualifier une action comme « malveillante » mais permettent d'identifier **des actions déviantes du comportement normal du système observé**.

Par exemple, ces algorithmes peuvent faire remonter des comportements inhabituels et donc potentiellement suspects tels que :

- un employé copiant brusquement un grand nombre de documents, qui peut indiquer une personne exfiltrant des documents avant de quitter l'entreprise ;
- le chiffrement massif de fichiers, qui peut indiquer le déploiement d'un ransomware dans un système d'information ;
- un employé qui utilise un logiciel qu'il n'a jamais utilisé auparavant, qui peut indiquer une compromission du poste ;
- un employé qui envoie des mails dans un format inhabituel, qui peut indiquer une tentative de propagation d'un malware ou d'extraction de données confidentielles.

[1] Le Mag IT, *Assises de la sécurité : Guillaume Poupard ne cache pas ses préoccupations*, Octobre 2019. lemagit.fr

Les logiciels d'analyse comportementale sont capables d'apprendre le fonctionnement habituel d'un système d'information : les habitudes de chaque employé, de chaque application, de chaque système industriel. Par exemple, la façon dont une personne travaille, sa manière de saisir les données, de rédiger ses mails, ses logiciels de bureautique et ses horaires. Ainsi, si lors d'une attaque, un malware ou un attaquant réussi à exploiter un compte utilisateur, ils ne pourront pas usurper cette empreinte personnelle et reproduire avec la même précision et la même spontanéité que l'utilisateur légitime ses habitudes et comportements individuels propres. Et ce d'autant que l'attaque elle-même implique de mener sur le système des actions qui ne sont pas les actions habituelles de l'utilisateur légitime. Ces actions provoquent alors un écart par rapport au comportement nominal de l'utilisateur légitime, et déclenchent une alerte.

Ainsi, grâce à cette approche, des comportement malveillants ou attaques qui n'ont jamais été qualifiées auparavant peuvent être identifiées et détectées.

Une nouvelle approche qui n'est pas sans contraintes

Le comportement normal d'un système est "appris" grâce à l'intelligence artificielle. Les logiciels d'analyse comportementale s'appuient donc sur les avancées de l'intelligence artificielle et notamment sur celles de l'apprentissage non supervisé, qui consiste à faire apprendre à la machine de manière automatique et autonome, sans étiquetage préalable des données. Leurs algorithmes établissent des liens entre des données dont on ignore si elles reflètent des comportements normaux et anormaux, et ces liens forment des modèles de comportement qui permettent de détecter tout comportement s'en éloignant et pouvant indiquer une action malveillante.

Cette approche nécessite donc à la fois un grand volume de données (qui implique que l'organisation qui souhaite déployer une telle solution dispose des données suffisantes), et un temps d'apprentissage significatif pouvant aller jusqu'à plusieurs semaines pour certains logiciels.

On peut alors considérer les limitations de cette approche. Pour être pleinement efficaces, ces technologies d'analyse comportementale doivent être déployées sur un système d'information sain, car, s'il est compromis, le logiciel considèrera comme normal le comportement de l'attaquant et le fait qu'il ait la main sur tout ou partie du système d'information. Ce qui constitue un véritable enjeu lorsque l'on sait que la détection des intrusions survient en moyenne 167 jours après la compromission initiale[2] et qu'il est donc tout à fait possible qu'une organisation déploie ce type de solutions sur un système déjà compromis. Elle rendrait par la même la solution inefficace au mieux, et au pire faciliterait l'action des attaquants déjà installés dans son système.

En outre, les fabricants sont parfois contraints d'installer des backdoors dans certains systèmes industriels pour intervenir à distance pour assurer la maintenance et la disponibilité de ces systèmes[3]. Dans ces cas-là également, le logiciel considèrera les actions à distance sur ces systèmes comme normales et diminuera ainsi la portée et l'efficacité de ces solutions d'analyse comportementale.

[2] Le Mag IT, *Détection d'intrusion : les chiffres très préoccupants relevés par Wavestone*, Octobre 2019. www.lemagit.fr
[3] FIC 2020, *Analyse comportementale, l'avenir de la détection ?*, janvier 2020.

Vers une approche hybride ?

L'analyse comportementale a donc des bénéfices très nets : capacité à traiter rapidement de très grands volumes de données, détection de modes opératoires inconnus… qui permettent aux SOC de dépasser des limites importantes des méthodes de détection historiques.

Mais il ne s'agit pas pour autant d'une solution miracle. Ces bénéfices sont acquis au prix de la clarté des remontées. Dans l'approche historique par signature statique, l'analyste sait qu'une détection d'intrusion est due à la présence d'un indicateur clairement identifié (adresse IP, hash, etc.) observé lors d'une opération précise suivant un mode opératoire bien identifié. L'analyse comportementale, en revanche, à un côté « boîte noire » : l'analyste ne sait pas précisément pourquoi, c'est-à-dire sur la base de quels indicateurs, l'algorithme considère qu'un comportement est anormal, sinon qu'il diffère d'un comportement habituel qualifié de normal.

Par ailleurs, certaines des contraintes de cette méthode, et notamment le temps d'entrainement des algorithmes, nécessitent d'importantes avancées technologiques pour être dépassées et permettre une efficacité optimale.

Une approche hybride de la détection, mêlant le meilleur des deux mondes – le travail de chercheurs et d'opérationnels de la cybersécurité, qui est au cœur de l'approche basée sur les signatures statiques, d'une part, et l'analyse des comportements grâce à l'intelligence artificielle de l'autre – permettrait de bénéficier des avantages des deux méthodes de détection. La méthode historique apporte une qualification explicite et précise des indicateurs, associée à de la construction de connaissance sur les modes opératoires des attaques là où l'analyse comportementale amène une identification plus rapide des anomalies, une augmentation des taux de détection et la découverte de circuits d'attaque qui étaient auparavant indétectables.

ANALYSES (2/2)

LA COURSE À L'INFORMATIQUE QUANTIQUE : ENTRE MYTHE ET RÉALITÉ

Les sciences de l'informatique quantique promettent de révolutionner la sécurité des communications et les capacités de calcul informatique. Elles visent à tirer parti des lois de la mécanique quantique, qui gouvernent le monde de l'infiniment petit et qui diffèrent de celles du monde macroscopique que nous connaissons. Parmi ces propriétés quantiques qui vont à l'encontre de notre logique intuitive, on retrouve notamment :

- La **superposition quantique** : une particule quantique peut être simultanément dans plusieurs états physiques contradictoires. Ainsi les « qbits » (pour « quantum-bit », la plus petite unité du système quantique), contrairement aux bits classiques qui sont des éléments binaires, peuvent à la fois être 0 et 1 ;
- L'**intrication quantique**, qui permet de lier les états de particules quantiques. Pour une paire de particules intriquées, tout changement d'état de l'une des particules provoque le changement d'état de l'autre, quelle que soit la distance les séparant. Le corollaire de cette intrication est la **téléportation quantique** : puisque les états de deux particules intriquées sont interdépendants, il devient possible de téléporter de l'information.

- La **décohérence quantique**, qui correspond à la fin de l'état de superposition quantique d'une particule et donc à la fixation de son état physique au sens classique. Ce phénomène de décohérence constitue le principal frein à l'ingénierie des dispositifs quantiques, celle-ci devant viser à éviter toute perturbation des particules.

Aujourd'hui, deux sous-domaines des sciences de l'information quantique intéressent particulièrement au niveau stratégique :

- L'**informatique quantique**, qui comprend le développement de calculateurs et d'algorithmes quantiques, avec des applications dans les domaines de la cryptanalyse, des simulations complexes (météorologie, armement, médecine, etc.) et du *big data* notamment ;
- La **cryptographie quantique**, qui vise à créer des réseaux de communications sécurisées.

Attirés par ces perspectives, de nombreux États sont progressivement entrés dans la course à l'informatique et aux communications quantiques.

L'informatique quantique : une nouvelle donne

L'engouement pour l'informatique quantique est véritablement né dans le milieu des années 90. Deux principaux algorithmes justifient la valeur stratégique du développement des calculateurs quantiques qui permettront de les exploiter.

En premier lieu, l'algorithme de Shor, proposé en 1994 par Peter Shor. Celui-ci propose une solution au phénomène dit « d'explosion combinatoire », c'est à dire le fait qu'un petit changement, même minime, du nombre de données à considérer dans un problème peut rendre sa solution très difficile, voire impossible, avec les ordinateurs actuels. En effet, avec un algorithme classique, la difficulté de résolution d'un problème combinatoire augmente de façon exponentielle avec chaque ajout de nouveau facteur. Un circuit de calcul quantique permet de réduire la vitesse d'augmentation de la difficulté du problème, celle-ci augmentant alors de façon polynomiale plutôt qu'exponentielle. L'application de l'algorithme de Shor par un calculateur quantique adapté, c'est-à-dire suffisamment dimensionné en termes de qbits, pourrait remplacer ou compléter les supercalculateurs traditionnels afin de :

- Améliorer le niveau d'automatisation de systèmes d'armement, en leur offrant une meilleure perception d'une situation avec l'augmentation de leur capacité à prendre en comptes des facteurs environnementaux supplémentaires ou d'en élargir la portée.
- Réaliser des simulations d'une complexité inatteignable avec l'informatique traditionnelle du fait de l'explosion combinatoire. L'application de cet algorithme permettra de franchir un cap dans le domaine de la recherche et de l'industrie civile et militaire, en favorisant l'utilisation de la simulation plutôt que la multiplication de prototypes et en réduisant ainsi le time-to-market.
- Briser la majeure partie des systèmes cryptographiques d'aujourd'hui, qui reposent sur une architecture asymétrique dont la résolution correspond à un problème de factorisation. Il deviendrait ainsi possible de calculer une clé privée à partir d'une clé publique, et ainsi de briser le secret des communications. Le risque et les niveaux d'investissement dans ce domaine sont considérés comme suffisamment sérieux pour que le développement d'algorithmes de chiffrement résistants à l'algorithme de Shor soit devenu une priorité et ait donné naissance à un nouveau domaine appelé « cryptographie post-quantique ». Dès 2016, la NSA signalait que les systèmes cryptographiques classiques ne devaient plus être considérés future-

proof et appelait au développement de nouveaux standards de chiffrement post-quantique par le NIST (*National Institute of Standards and Technology*), qui a lancé son programme de standardisation quantique mais qui, dans l'attente de premiers drafts prévus pour 2022, appelle les organisations à la « crypto-agilité », c'est à dire elles doivent faire au mieux pour se préparer à migrer au plus tôt vers les futurs standards.

L'autre algorithme majeur est celui proposé par Lov Grover en 1996. Il constitue l'algorithme le plus efficace pour rechercher des informations au sein de bases de données non structurées, ce qui le rendrait particulièrement efficace dans le domaine du *big data* et de l'apprentissage automatique. L'algorithme de Grover pourrait également permettre de briser les chiffrements symétriques, mais la simple augmentation de la taille des clés de chiffrement symétriques pourrait être une réponse suffisante.

Le développement réussi de calculateurs quantiques capables d'appliquer ces algorithmes propulserait ainsi les capacités économiques, scientifiques et militaires des pays bénéficiaires, ce qui explique l'engouement actuel pour la recherche dans ce domaine.

La cryptographie quantique : la recherche d'une sécurité infaillible

La cryptographie quantique vise à établir un canal de communication sécurisé permettant de faire transiter des particules quantiques porteuses d'information. En raison de la difficulté du maintien de la cohérence quantique des particules, les applications actuelles ne visent pas à faire transiter de vastes quantités d'information, mais uniquement les clés de chiffrement qui permettront de sécuriser des communications qui emploieront des canaux de communication classiques. Ces derniers restent d'ailleurs nécessaires à l'échange de clés pour des raisons qui tiennent aux protocoles des échange de clés, Ainsi, tout canal de communication quantique est nécessairement doublé d'un canal classique, sécurisé, au moins pour le premier échange de clés quantiques, par un protocole de chiffrement classique.

C'est le phénomène de décohérence quantique qui assure la sécurité des échanges : lors de l'échange d'une clé de chiffrement sur un canal quantique, toute tentative de mesure prématurée, par exemple par une tentative malicieuse d'interception sur le trajet, par un tiers perturberait les particules quantiques échangées, qui ne pourraient donc plus être lues à l'arrivée par les destinataires/ interlocuteurs légitimes.

Deux principaux canaux d'échange de particules quantiques sont employés ou envisagés aujourd'hui :

- Les fibres optiques, qui permettent l'échange de clés sur une distance de l'ordre de la centaine de kilomètres. Le phénomène d'atténuation des fibres optiques limite cette distance maximale, et l'emploi de relais, en qui il faut donc accorder confiance, est nécessaire pour prolonger les communications. Ces relais convertissent l'information quantique en information « classique » et re-génèrent une clé pour la portion suivante. Des systèmes de véritables répéteurs équipés de mémoire quantiques, encore à l'étape de recherche, devraient permettre à terme d'assurer une véritable liaison quantique sur de grandes distances sans passer par des relais ;
- Les communications quantiques satellitaires, qui devraient permettre d'augmenter considérablement la distance maximale d'échanges pour atteindre plusieurs milliers de kilomètres.

L'informatique quantique, enjeu de rivalités industrielles et commerciales internationales

Les communications quantiques filaires sont une réalité commerciale depuis les années 2000. Des dispositifs commerciaux de distribution de clé quantiques, ou QKD (*Quantum Key Distribution*) sont d'ores et déjà déployés et utilisés, notamment par des institutions financières, des universités et des organisations gouvernementales. Ils utilisent des liaisons par fibre optique, parfois mises en place spécifiquement, mais il est également possible de reconvertir des réseaux fibrés préexistants, pour peu qu'ils soient dédiés à cette tâche. Ces liaisons permettent des communications point à point d'une portée d'une centaine de kilomètres, mais des systèmes de relais quantiques permettent de couvrir des distances plus vastes, à l'instar du lien déployé entre Beijing et Shanghai en 2016 (soit 2 000 km)[4].

Le satellitaire quantique : la Chine en tête

Si de nombreux pays possèdent des acteurs commerciaux sur ce créneau des liaisons quantiques terrestres, la Chine possède une avance considérable dans le domaine satellitaire quantique. La Chine, qui mène depuis 2003 des expériences dans le domaine de la téléportation quantique à l'Académie chinoise des sciences (ACS), a intégré en 2011 le programme QUESS (*Quantum Experiments at Space Scale*) à son 12ème plan quinquennal. Celui-ci, qui intègre une coopération avec l'*Institute for Quantum Optics and Quantum Information* de Vienne, vise à développer un système satellitaire permettant des communications chiffrées inviolables sur de grandes distances[5]. Un premier satellite a ainsi été lancé en 2016. En 2017, ce satellite qui vole à plus de 8 km/s a réalisé une première transmission d'une paire de photons intriqués entre les stations terrestre de Delingha (plateau tibétain) et l'observatoire Gaomeigu à Lijiang, soit plus de 1 200 km. La Chine prévoyait un réseau euroasiatique d'ici 2020 mais il semblerait que les tests soient encore en cours, à l'aide du premier satellite réalisé avec l'université de Vienne. Un réseau mondial est également prévu d'ici 2030.

Les calculateurs quantiques : les États-Unis en avance

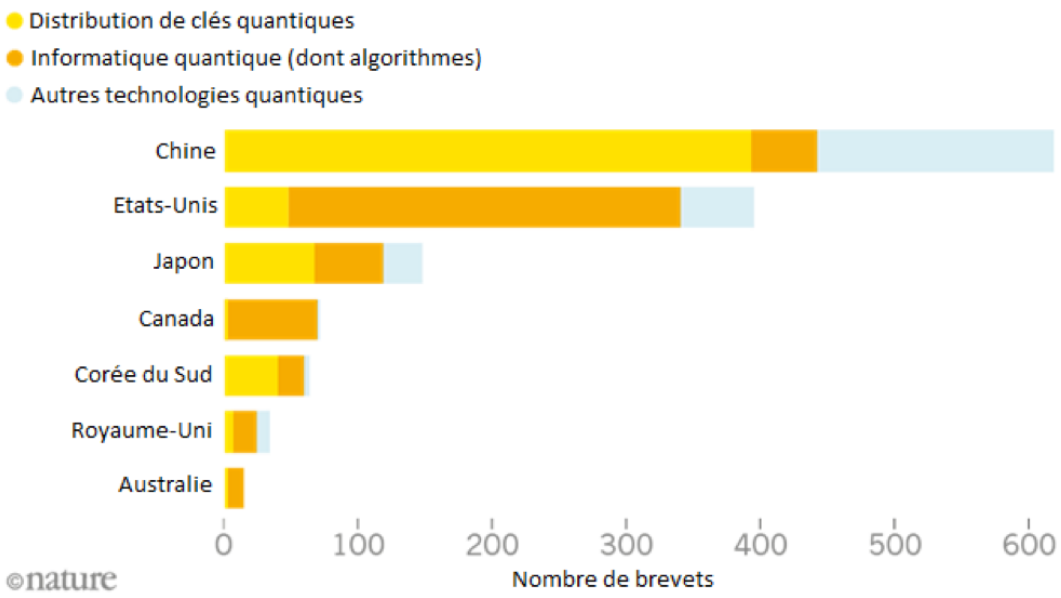
Du côté des calculateurs quantiques en revanche, les États-Unis semblent avoir développé une nette avance à travers ses grandes entreprises du numérique. Le pays maintien des liens commerciaux forts avec l'entreprise canadienne D-Wave Systems, qui a été la première à réussir à développer un calculateur quantique commercial, bien que non généraliste et dédié à la résolution des problèmes d'optimisation. IBM et Google travaillent quant à eux sur le développement d'ordinateurs quantiques généralistes. Le premier met par exemple à disposition des chercheurs du monde entier un ordinateur quantique afin qu'ils puissent tester leurs algorithmes, à conditions qu'ils en offrent la propriété à l'entreprise américaine… Google, quant à elle, a récemment annoncé avoir atteint la suprématie quantique, en réalisant un calcul plus rapidement que ne le pourrait un ordinateur classique[2].

[4] https://spectrum.ieee.org/telecom/security/chinas-2000km-quantum-link-is-almost-complete

[5] Le principe est le suivant : un satellite produit des paires de photons intriqués, dont chacun est envoyé à une différente station au sol. Du fait de la corrélation quantique de ces particules, la mesure d'un photon par l'une de ces stations fixe l'état des deux photons. Il s'agit d'une téléportation quantique qui permet d'échanger de l'information sans que celle-ci ait eu besoin de transiter entre les deux stations.

La course au quantique, une compétition mondiale

L'enregistrement des brevets montre bien cet état de fait d'une nette avance de la Chine dans le domaine des communications quantiques, en opposition à la nette avance américaine sur l'informatique quantique[6].



Brevets enregistrés depuis 2012, d'après une étude de la commission européenne menée par Martino Travagnin.

Source : Nature

La Chine et les États-Unis ont donc au cours de la précédente décennie opté pour des investissements diamétralement opposés dans les technologies de l'information quantique. Alors que les États-Unis faisaient partie des pionniers des réseaux de communication quantique avec la DARPA, elle a laissé la Chine les rejoindre puis les dépasser nettement. La Chine sera selon toute vraisemblance le premier pays à posséder un réseau opérationnel de communication quantique satellitaire mondial, alors qu'il semble que les calculateurs quantiques sont encore à des décennies de porter véritablement leurs fruits. Elle entend cependant rattraper son retard dans ce domaine, avec un investissement inédit de 10 milliards de dollars dans la création du *National Laboratory for Quantum Information Sciences* qui concentrera ses recherches dans deux domaines : les calculateurs quantiques et la métrologie quantique[7,8]. De même aux États-Unis, au-delà des investissements massifs portés par les grandes entreprises du numérique, le gouvernement n'est pas en reste avec la récente signature du *National Quantum Initiative Act*, qui prévoit un investissement de 1,2 milliards de dollars sur 5 ans dans les technologies de l'information quantique.

De son côté, l'Union Européenne a officiellement lancé en 2018 l'initiative *Quantum Flashship*, dotée d'un budget d'un milliard d'euros sur 10 ans, dont 132 millions sur les trois premières années. Elle vise à développer la recherche et à démarrer une industrie dans les domaines d'application de la physique quantique

[6]https://publications.jrc.ec.europa.eu/repository/bitstream/JRC115251/patent_analysis_of_selected_quantum_technologies_1.pdf

[7] https://www.popsci.com/chinas-launches-new-quantum-research-supercenter/

[8] La métrologie quantique vise à repousser les niveaux de précision de mesure (masse temps, courant électrique, etc.).

(communications, informatique, simulation et métrologie). Ce projet s'ajoute aux initiatives individuelles des pays membres de l'UE, bien qu'il soit difficile de distinguer les financements intégrés à l'initiative européenne de celles qui relèvent de l'initiative privée. Les investissements dans le cadre du *National Quantum Technologies Programme* du Royaume-Uni ont quoiqu'il en soit dépassé en 2019 le milliard de livres[9], alors que dans le même temps l'Allemagne projette d'investir 650 millions d'euros sur deux ans dans les travaux de recherche menés par IBM[10] (plutôt que de l'européen Atos…), et que d'autres États membres dont la France investissent à des niveaux compris en 50 et 150 millions d'euros.

Parmi les autres principaux pays investissant massivement dans le secteur, on peut citer le Canada qui a investi plus d'un milliard de dollars au cours de la décennie et semblait être en position de leader avec les avancées de l'entreprise D-Wave, la Russie qui prévoit d'investir 790 millions sur les 5 prochaines années[11], ou encore l'Inde qui souhaite aujourd'hui rejoindre la course avec un investissement de 1.12 milliards de dollars sur 5 ans[12].

Vers un « hiver quantique » ?

On peut se demander si la frénésie actuelle autour de ces technologies ne risque pas de donner lieu à un « hiver quantique », similaire aux « hivers » de l'intelligence artificielle, dont la recherche a connu plusieurs épisodes de surinvestissements suivis d'assèchement des crédits durant de nombreuses années lorsque les résultats ne se sont pas montrés à la hauteur des promesses. La revue Nature note ainsi un signe inquiétant : une part significative des investissements soutient des initiatives de développement d'algorithmes quantiques, pour lesquels il n'existe pourtant encore aucun calculateur quantique permettant de les appliquer[13]. De même, la suprématie quantique qu'a revendiqué Google ne correspondait qu'à la résolution d'un problème sans réelle application autre que la démonstration de cette capacité, et les scientifiques considèrent que les calculateurs quantiques généralistes devront réunir un minimum d'un million de qbits pour avoir une réelle utilité, alors que les meilleurs calculateurs actuels en réunissent quelques dizaines au maximum, et que la difficulté de maintien de la cohérence quantique augmente exponentiellement avec le nombre de qbits.

Du côté des réseaux de communication quantiques, bien que des dispositifs commerciaux existent et la recherche du côté spatial semble être en bonne voie, il faut reconnaître leurs limitations : dans tous les cas, on doit doubler le canal quantique d'un canal classique ; au sol, la portée limitée du signal implique la multiplication de répéteurs de confiance ; dans l'espace enfin, les faibles orbites actuellement nécessaires à la réussite des transmissions impliquent des fenêtres d'échange très courts (quelques minutes à peine). D'autre part, la fragilité inhérente aux particules quantiques, si elles permettent d'apporter une assurance de sécurité, les rendent également potentiellement particulièrement vulnérables à des attaques en déni de service.

[9] https://www.gov.uk/government/news/1-billion-investment-makes-uk-a-frontrunner-in-quantum-technologies

[10] https://www.fraunhofer.de/en/press/research-news/2020/march/ibm-and-fraunhofer-bring-quantum-computin-to-germany.html

[11] https://www.nature.com/articles/d41586-019-03855-z

[12] https://www.nature.com/articles/d41586-020-00288-x

[13] https://singularityhub.com/2019/10/14/investment-in-quantum-computing-is-booming-but-will-a-quantum-winter-follow/

Conclusion

Il est certain que les sciences de l'information quantique apporteront à ceux qui les maîtriseront des gains considérables dans tous les secteurs, de façon similaire aux gains apportés à l'informatique classique. Il reste à espérer que les efforts consentis en matière d'investissement le soient avec une vision à très long terme de sorte qu'ils ne disparaissent pas malgré la relative lenteur des progrès. Cela correspond à l'horizon temps d'un Etat, mais peut-être moins des Hedge funds qui ont commencé à se pencher sur le secteur. Ces derniers sont particulièrement intéressés par les applications potentielles pour leur cœur de métier, mais se retireront soudainement si la confiance en un développement rapide venait à se perdre ?

FOCUS INNOVATION

COUNTERCRAFT : LA CYBER « DECEPTION » ACTIVE

Entretien avec David Barroso, fondateur.

Présentation

Cofondée en 2015, la société CounterCraft est présente à Londres, Madrid et Los Angeles, et mène ses activités de R&D à San Sebastián, en Espagne. Les fondateurs de la société, issus du milieu de la cybersécurité, souhaiter créer une solution de « cyber deception », c'est-à-dire décéptive, ou « de tromperie » innovante et « active » pour fournir les outils nécessaires pour lutter contre l'espionnage et les attaques avancées, difficiles à détecter et à suivre par les organisations. Son portefeuille client compte des organisations des secteurs gouvernementaux, de la défense, de la finance, de l'énergie et du e-commerce. CounterCraft compte plusieurs références stratégiques sur tout le continent européen comme américain, sur des secteurs sensibles comme le militaire, la finance et l'industrie. CounterCraft est installé en France depuis Septembre 2019 et a confié son implantation à NEOSMOS

CounterCraft a reçu 3 millions d'euros de financement de la part d'investisseurs européens spécialisés dans la cybersécurité et a reçu 1 million d'euros de financement par le programme de recherche et d'innovation Horizon 2020 de l'Union européenne (convention de subvention n ° 767383).

Countercraft a également reçu le prix américain "New Generation Cyber Deception" pour sa solution innovante et a été reconnue "Best Buy in Deception Technology" par SC Magazine UK en juin 2019.

La solution

La solution de cyberdeception de CounterCraft permet de mettre en place des environnements simulés, c'est-à-dire de reproduire des systèmes d'informations afin d'y attirer les attaquants et ainsi de détecter en temps réel les attaques ciblées. Ce dispositif permet par la même d'identifier le point d'entrée des attaquants, et d'observer et comprendre leur mode opératoire, leurs outils, ainsi que leurs techniques et tactiques.

La solution s'intègre aux stratégies de sécurité de ses clients et fournit des renseignements exploitables sur l'attaquant (méthodologies, déplacements dans le SI, outils utilisés, TTPS…) pour faciliter la détection précoce des menaces et limiter le temps de réponse à incident. Le modèle de déploiement de sa plateforme de

cyberdeception permet de créer des campagnes de déception sur plusieurs types de ressources tels que des réseaux locaux, externes, des clouds, etc…

Countercraft permet de détecter tous types d'attaque et à tous les stades de l'incident, à la fois bien en amont dès le stade de la reconnaissance passive en vue d'une intrusion, mais aussi plus tard lorsque les attaquants sont déjà présents sur le système d'information de l'organisation.

L'innovation

L'activité de l'attaquant (évènements, phases de l'attaque) peut être entièrement visualisée en temps réel de manière graphique et chronologique via un dashboard pour faciliter l'analyse et la réponse à incident. Des fonctionnalités de filtrage et d'analyse automatique des données permettent d'identifier et de marquer les activités malveillantes identifiées en fonction des indicateurs de compromission (IoCs) et des TTPs connus utilisés.

Pour être crédible et attirer l'attaquant sans qu'il ne se rende compte qu'il est surveillé, la plateforme lui donne accès, via l'environnement simulé, à des informations ayant l'apparence des données sensibles de ses cibles. Celles-ci sont en fait protégées car les systèmes d'information restent cloisonnés, l'environnement simulé constituant ainsi une "zone de sécurité" dans laquelle les attaquants n'ont pas accès au véritable système d'information de l'organisation ciblée.

La plateforme de CounterCraft se démarque des solutions de cyberdeception classiques en ce qu'elle permet trois fonctionnalités : la détection de l'attaque, l'investigation sur l'attaque, et l'interaction en temps réel avec les attaquants.

- **Détection** : La solution détecte la présence d'attaquants de manière discrète de façon à ce que les attaquants n'aient pas conscience de faire l'objet d'une surveillance.
- **Investigation** : CounterCraft analyse et surveille les attaques en temps réel, grâce à sa plateforme qui capture et identifie automatiquement les TTPs des attaquants sur la base du cadre MITRE ATT&CK. Les données sont enrichies par des ressources Open Source de Threat Intelligence des analystes de Countercraft, et sont régulièrement mises à jour en fonction de l'état et de l'évolution de la menace. Ce dispositif permet d'analyser l'activité de l'adversaire de manière très détaillée, et de produire un renseignement sur la menace locale contextualisé, ciblé et exploitable.
- **Interaction** : La plateforme délivre, temps réel, des alertes et des actions contextualisées à l'équipe de sécurité de l'organisation ciblée. Elle permet également de concevoir et déployer, toujours en temps réel, des campagnes de « déception » afin d'influencer les choix de l'attaquant à mesure qu'il croit progresser dans le SI ciblé. L'équipe de sécurité peut ainsi prolonger l'interaction avec l'attaquant pour recueillir davantage de données sur son activité et son mode opératoire. Elle permet enfin de de générer des données d'analyse utilisées pour prévoir les prochaines étapes de l'attaque. Les activités de l'attaquant sont enregistrées et transmises de manière sécurisées à l'équipe de sécurité. Toutes les données relatives à l'activité de l'adversaire sont mises à disposition de l'organisation ciblée à partir de la plateforme de Countercraft via l'API RESTful, exportable à l'aide de protocoles de partage (STIX2 ou OpenIOC) vers une plateforme MISP ou vers un SIEM.

À terme, Countercraft souhaite étendre son offre à l'analyse prédictive, en travaillant sur les modèles d'attaques.

ACTUALITÉ

ÉTATS-UNIS : PUBLICATION DU RAPPORT DE LA CYBERSPACE SOLARIUM COMMISSION

Le 11 mars 2020, la commission parlementaire américaine « Cyberspace Solarium Commission » a rendu public son rapport portant sur le développement d'une approche stratégique commune des institutions fédérales pour lutter contre les cyberattaques et leurs conséquences[14]. Le travail de la Commission s'est notamment intéressé à relever les contradictions existantes dans la stratégie cyber américaine et à améliorer les efforts du gouvernement fédéral pour atteindre ses objectifs stratégiques dans le cyberespace[15].

Le rapport préconise la mise en œuvre d'une stratégie de cyber-dissuasion en plusieurs couches (*strategy of layered cyber deterrence*) avec pas moins de 80 recommandations portant sur 6 piliers stratégiques :

- La réforme des institutions gouvernementales liées au cyberespace ;
- Le renforcement des normes applicables au cyberespace et aux mécanismes non militaires de règlement des conflits ;
- La promotion d'une résilience nationale cyber ;
- La remodélisation de l'écosystème cyber ;
- La coopération opérationnelle entre les secteurs public et privé en matière de cybersécurité ;
- Sur le maintien et l'emploi des capacités militaires en matière cyber.

À travers ses recommandations, le rapport parlementaire réaffirme la stratégie « *defend forward* » (« arrêter la menace avant qu'elle n'atteigne sa cible[16] ») adoptée par le Département de la défense américaine (DOD) en 2018[17] en la plaçant au service de la stratégie plus globale de cyber-dissuasion en plusieurs couches. Concrètement, cette dernière se déclinerait en 3 couches appliquant la stratégie « *defend forward* » en fonction du niveau de conflictualité :

- La première couche concerne la régulation des comportements dans le cyberespace et les mécanismes de coopération internationale pour lutter contre la cybercriminalité ou encore la prolifération des cyberopérations ;
- La seconde couche concerne les mesures de sécurité contre les cyberattaques contre les infrastructures vitales ou les élections par exemple ;
- La troisième couche concerne l'utilisation des capacités militaires cyber.

---

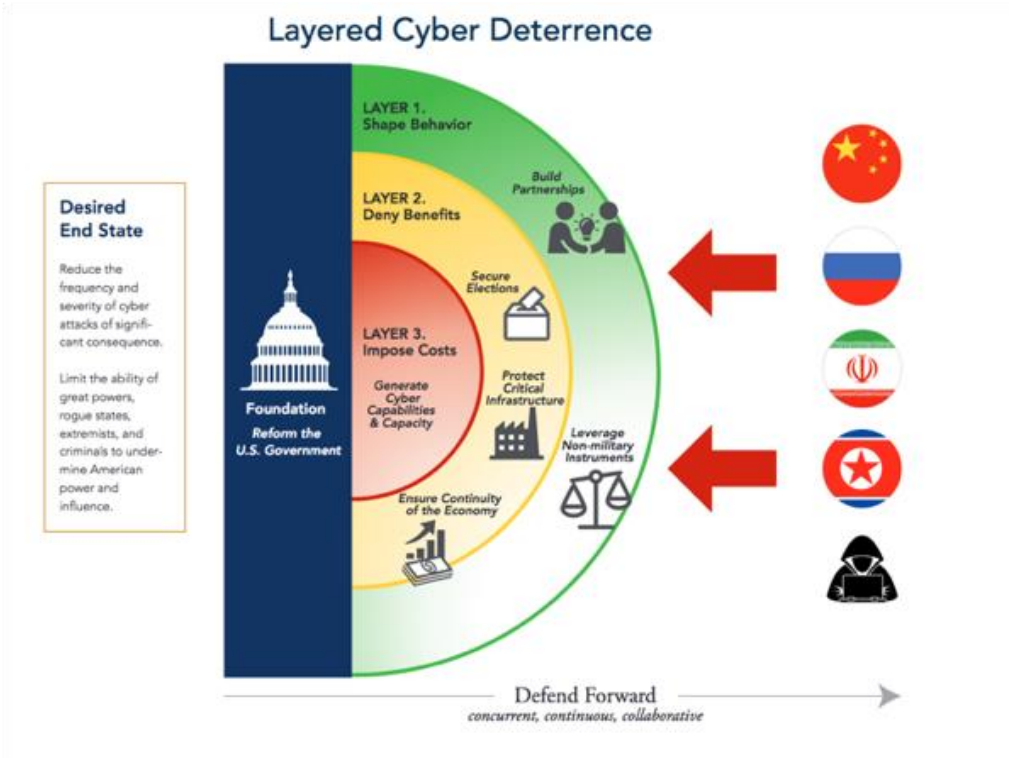
[14] https://www.solarium.gov/home

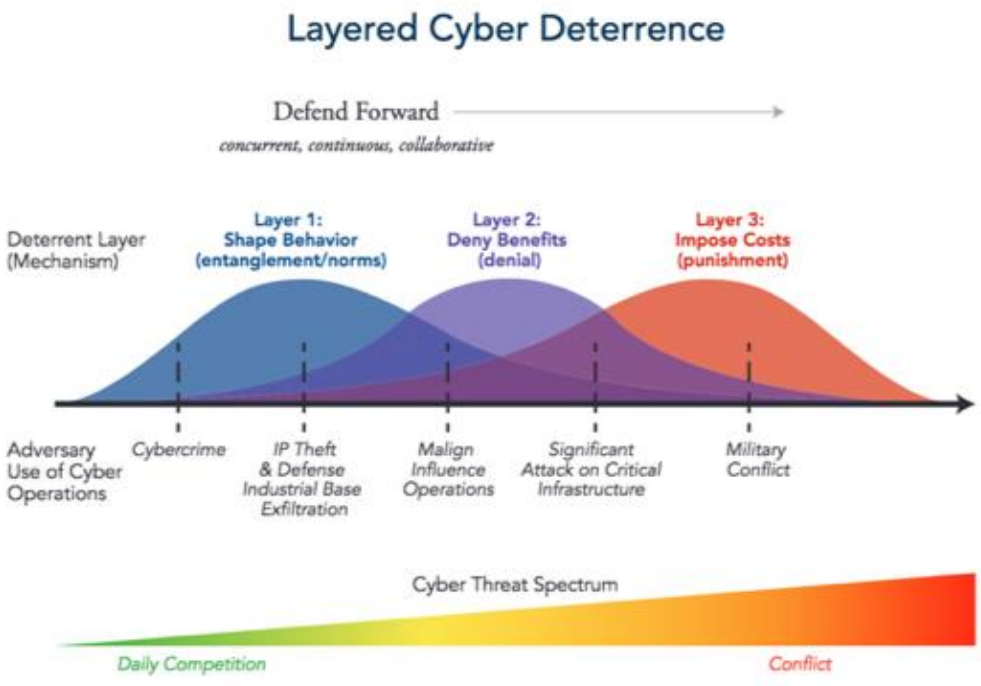
[15] https://www.lawfareblog.com/cyberspace-solarium-commission-competing-complementary-strategies

[16] https://www.irsem.fr/data/files/irsem/documents/document/file/2959/N%C2%B0198%20-%20Note%20-%20La%20nouvelle%20strat%C3%A9gie%20cyber%20des%20%C3%89tats-Unis.pdf

[17] https://www.lawfareblog.com/cyberspace-solarium-commission-report-and-persistent-engagement ; https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Schémas de la stratégie de cyber-dissuasion sur plusieurs couches[18]





[18] https://s.wsj.net/public/resources/documents/CSC%20Final%20Report.pdf?mod=article_inline

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.

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 – 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